MA3265 Introduction to Number Theory

Notes by Chan Heng Huat for NUS-AY2021/2022 Semester 2

Contents

References

The main reference is "An introduction to the theory of numbers" by I. Niven, H.S. Zuckerman and H.L. Montgomery. Most of the tutorial problems in this course can be found in the book.

Other references are "Elementary Number Theory" by D. Burton, "A course in arithmetic" by J.P. Serre, "Primes of the form $x^2 + ny^2$" by D.A. Cox, "Introduction to Analytic Number Theory" by T.M. Apostol, "Introduction to Number Theory" by D. Flath, "Elementary Theory of Numbers" by W. Sierpinski (with second edition edited by A. Schinzel), "Number Theory" by G.E. Andrews and "Introduction to the theory of numbers" by G.H. Hardy and E.M. Wright.

1 Divisibility

1.1 Introduction

Number Theory is a branch of mathematics that study problems involving integers

$$\mathbf{Z} = \{0, \pm 1, \pm 2, \pm 3, \cdots\}.$$

We list several examples of such problems.

DEFINITION 1.1 An integer s is called a *perfect square* if it is of the form $s = m^2$ for some integer m.

EXAMPLE 1.1 Determine all integers which can be expressed as a sum of two perfect squares.

EXAMPLE 1.2 Determine the most general solutions of $x^2 + y^2 = z^2$ where $x, y, z \in \mathbf{Z}$.

REMARK 1.1 The triplet (x, y, z) with $x, y, z \in \mathbf{Z}$ satisfying $x^2 + y^2 = z^2$ is called a *Pythagorean triplet*.

EXAMPLE 1.3 Let $n \geq 3$. There is no three positive integers x, y and z that satisfy the equation $x^n + y^n = z^n$.

REMARK 1.2 This is the *Fermat Last Theorem*. It was proved by A. Wiles and R. Taylor in 1995.

DEFINITION 1.2 Let a and b be two integers such that $ab \neq 0$. We say that a is a *divisor* of b if $b = aq$ for some integer q. We use the notation $a|b$ to mean a divides b. We also say that a is a *factor* of b and that b is a *multiple* of a.

DEFINITION 1.3 A *prime number* is a positive integer with exactly two positive divisors. An integer $n > 1$ which is not a prime is called a *composite number*.

There are many interesting problems (some of which are unsolved) that are related to prime numbers. We list a few here.

EXAMPLE 1.4 Are there infinitely many primes?

DEFINITION 1.4 The symbol $\pi(x)$ denote the number of primes less than x.

EXAMPLE 1.5 The prime number theorem states that

$$\lim_{x\to\infty} \frac{\pi(x)}{(x/\ln x)} = 1.$$

REMARK 1.3 This is the *Prime Number Theorem*. It was first observed by C.F. Gauss around 1791 and A.M. Legendre around 1798. It was proved independently around 1896 by J. Hadamard and Charles de la Vallée Poussin using complex analysis. Elementary proofs of this result without using complex analysis were later given by A. Selberg and P. Erdös around 1948. Both proofs required the Selberg identity. Since the appearance of the proofs by Selberg and Erdös, other elementary proofs were discovered. Some of these proofs were independent of Selberg's identity and one of the most elegant proofs was given in 1986 by A. Hildebrand using the theory of large sieve.

DEFINITION 1.5 We say that two integers a and b are *relatively prime* if there does not exist an integer $c > 1$ such that $c|a$ and $c|b$.

EXAMPLE 1.6 Suppose a and b are two relatively prime positive integers. Are there infinitely many primes of the form $an + b$?

REMARK 1.4 This is known as *Dirichlet's Theorem of primes in arithmetic progression.*

There are many other problems besides those stated here. Some of these problems are solved while others remained open. In this course, we will study some basic results in various areas of number theory. Hopefully by the end of this course, students will be able to appreciate the relations among different areas of mathematics through solving number theoretic problems and that they will be able to appreciate the beauty of number theory, the "queen of mathematics".

1.2 Division algorithm and congruences

We have seen in Definition 1.2 that if a is a divisor of b, we write $a|b$. When a is not a divisor of b, we use the notation $a \nmid b$.

THEOREM 1.5 Let a, b, c, x, m, y be integers.

(a) $a|b$ implies that $a|bc$ for any integer c;
(b) $a|b$ and $b|c$ imply $a|c$;
(c) $a|b$ and $a|c$ imply $a|(bx + cy)$ for any integers x and y;
(d) $a|b$ and $b|a$ imply $a = \pm b$;
(e) $a|b$, $a > 0$, $b > 0$, imply $a \leq b$;
(f) Let m be a nonzero integer. Then $a \mid b$ implies that $am \mid bm$; if $am \mid bm$, then $a \mid b$.

Proof

We prove (c). Suppose $a \mid b$ and $a \mid c$, then $b = ak$ and $c = al$ for some integers k and l. Now,

$$bx + cy = a(kx + ly).$$

Hence $a|(bx + cy)$. □

THEOREM 1.6 (The Division Algorithm) Given any integers a and b with $a > 0$, there exist unique integers q and r such that $b = qa + r, 0 \leq r < a$. If $a \nmid b$, then r satisfies the stronger inequalities $0 < r < a$.

To prove the above result, we will first need the least integer axiom, which says that if S is the nonempty subset of positive integers, then there is an element $r \in S$ such that $r \leq s$ for all $s \in S$. This principle cannot be proved but it is certainly plausible. Suppose 0 is not in S, then 0 is not the smallest element in S. If 1 is not in S, then 1 is not the smallest element in S. Since S is nonempty, then there must be an integer r that happens to be the first integer in S. This integer r is the smallest integer in S.

REMARK 1.7 One can show that the least integer axiom is equivalent to the mathematical induction.

We are now ready to prove the Division Algorithm.

Proof

First, note that if $a|b$, then $r = 0$. Suppose $a \nmid b$. Let

$$S = \{y : y = b - ax, \ \ x \text{ is an integer}, \ y \geq 0\}.$$

Note that since $a \geq 1$ and

$$b - a \cdot (-2|b|) = |b| \left(\frac{b}{|b|} + 2a \right) > |b| \left(\frac{b}{|b|} + 2 \right) > 0,$$

we see that S is non-empty. By the least integer axiom, it has a smallest member, say $r = b - aq$. Then $b = aq + r$ and $r \geq 0$. Now we show that $r < a$.

Suppose $r \geq a$. Then $0 \leq r - a = b - a(q+1)$ and hence $r - a \in S$. Since $r - a < r$, this contradicts the minimality of r. Hence, $r < a$. The pair q, r is unique, for if there is another pair q', r' such that $b = aq' + r'$, then $a(q' - q) = r - r'$. If $r = r'$, then $q = q'$ and we complete the proof of the Theorem. Suppose $r \neq r'$. Then $|r - r'| > 0$ and $a \,|\, |r - r'|$. By Theorem 1.5(e), we find that

$$|r - r'| \geq a. \tag{1.1}$$

But $0 \leq r' < a$ implies that $-a < -r' \leq 0$. Together with $0 \leq r < a$, we conclude that

$$-a < r - r' < a,$$

or

$$|r - r'| < a.$$

This contradicts (1.1). □

REMARK 1.8 If we let $a = 2$ in Theorem 1.6, then our conclusion is that every integer is of the form $2k$ or $2k+1$. If we let $a = 4$, then we find that every integer is of the form $4k, 4k + 1, 4k + 2$ or $4k + 3$.

EXAMPLE 1.7 Show that if n is of the form $4k + 3$ then n is not a perfect square.

Solution

Let m be any integer. Then m is of the form $4k+j, 0 \leq j \leq 3$. This implies that m^2 is of the form $4k$ or $4k+1$. Therefore, a square can only be of the form $4k$ or $4k+1$.

EXAMPLE 1.8 Show that if n is of the form $4k+3$, then n is not a sum of two squares.

Solution

A square is of the form $4k$ or $4k+1$. Therefore, a sum of two squares can only be of the form $4k, 4k+1$ or $4k+2$. In other words, if n is of the form $4k+3$, it cannot be a sum of two squares.

REMARK 1.9 The above example shows that if p is a prime of the form $4k+3$ then it is not a sum of two squares. Since an odd prime is either of the form $4k+1$ or $4k+3$, it is natural to ask whether a prime of the form $4k+1$ is always a sum of two squares. The answer to this question is yes and in this course, we will see several proofs of this fact.

We now introduce congruences.

DEFINITION 1.6 Let $n > 0$ be an integer. We say that "a is congruent to b modulo n" and write

$$a \equiv b \pmod{n}$$

if

$$n|(a-b).$$

With the above notation, we can replace the sentence "Every integer n is of the form $2k$ or $2k+1$." by "Every integer n is such that $n \equiv 0$ or $1 \pmod 2$.".

DEFINITION 1.7 Let $n \geq 2$ be a positive integer. Define $[j]_n = \{k | k \equiv j \pmod{n}\}$.

The Division Algorithm shows us that the set of integers

$$\mathbf{Z} = \bigcup_{j=0}^{n-1} [j]_n.$$

REMARK 1.10 It is known that the set $A(n) = \mathbf{Z}/n\mathbf{Z} = \{[r]_n | 0 \leq r < n\}$ forms a group under the operation $[a]_n + [b]_n = [a+b]_n$.

We now list a few basic properties of congruences.

THEOREM 1.11 Let a, b, c, d, n be integers with $n > 0$. Then

(a) For all integers k, $k \equiv k \pmod{n}$.
(b) If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$.
(c) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$.
(d) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$.

We will only supply the proof of Theorem 1.11 (d).

Proof of Theorem 1.11 (d)
Since $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, we deduce that $n|(a-b)$ and $n|(c-d)$. Hence, $a - b = nk$ and $c - d = nj$. Therefore, $a + c = b + d + n(k + j)$, which implies that $n|(a + c) - (b + d)$, i.e., $a + c \equiv b + d \pmod{n}$. Now, $a = nk + b$ and $c = nj + d$ also implies that $ac = bd + n(kd + bj + nkj)$. Hence $ac \equiv bd \pmod{n}$. □

The use of congruences allow us to have shorter presentations of solutions to the next few problems.

EXAMPLE 1.9 Show that 3 divides $a(2a^2 + 7)$ for any integer $a \in \mathbb{Z}$.

Solution

Let a be any integer. Then $a \equiv 0, 1$ or $2 \pmod{3}$. This implies that

$$a(2a^2 + 7) \equiv 0 \cdot 7, 1 \cdot 9 \text{ or } 2 \cdot 15 \pmod{3}.$$

In all cases, $a(2a^2 + 7) \equiv 0 \pmod{3}$ and hence $3|a(a^2 + 2)$.

EXAMPLE 1.10 Show that if p is an odd prime of the form $4k+3$ then p is not a sum of two squares.

Solution

We have seen that a square is congruent to 0 and 1 modulo 4. Hence a sum

of two squares must be congruent to 0,1 or 2 modulo 4. This means that any integer of the form $4k+3$ cannot be a sum of two squares. In particular, a prime of the form $4k+3$ is not a sum of two squares. This completes our solution of the problem.

Now, since an odd prime is either of the form $4k+1$ or $4k+3$, it is natural to determine if primes of the form $4k+1$ were a sum of two squares. It turns out that this is always true. We will see proofs of this result in subsequent chapters.

EXAMPLE 1.11 Show that $41|(2^{20}-1)$.

Solution

Note that $2^{10} = 25 \cdot 41 - 1$. Therefore $2^{10} \equiv -1 \pmod{41}$ and $2^{20} \equiv 1 \pmod{41}$.

1.3 Greatest Common Divisors

Let a and b be integers such that a and b are not simultaneously equal to 0.

DEFINITION 1.8 A *common divisor* of integers a and b is an integer c with $c|a$ and $c|b$.

DEFINITION 1.9 A *greatest common divisor* of integers a and b is an integer d with the following properties :

(a) The integer d is positive.
(b) The integer d is a common divisor of a and b.
(c) If e is any common divisor of a and b, then $e|d$.

Note that if d and d' are both greatest common divisors of a and b, then d is a common divisor of a and b and d' is a greatest common divisor, we note that $d'|d$ using Definition 1.9 (c). Similarly, since d' is a common divisor and d is a greatest common divisor, $d|d'$. By Theorem 1.5 (d), $|d| = |d'|$ and by Definition 1.9 (a), we deduce that $d = d'$. This shows that the greatest common divisor of a and b is unique.

DEFINITION 1.10 The notation we use for the greatest common divisor of a and b is (a, b).

REMARK 1.12 If $a = 0$ and b is non-zero, then $(0, b) = |b|$.

We will next show that the greatest common divisor of two integers exists. By Remark 1.12, it suffices to consider the case when both a and b are nonzero.

THEOREM 1.13 Let a and b be nonzero integers. Then the smallest positive integer in the set

$$P := \{sa + tb | s, t \in \mathbf{Z} \quad \text{and} \quad sa + tb > 0\}$$

is (a, b).

Proof
If a is positive then $a \in P$ since

$$a = 1 \cdot a + 0 \cdot b.$$

Similarly, if b is positive, then $b \in P$. Suppose a and b are both negative. Then $0 \cdot a + (-1) \cdot b \in P$. Hence that P is nonempty. By the least integer axiom, there is a smallest positive integer, say d, in P. We must show that $d = (a, b)$.

We observe that $d \geq 1$ since we have assumed that both a and b are nonzero. Next, since $d \in P$,

$$d = xa + yb \tag{1.2}$$

for some integers $x, y \in \mathbf{Z}$. We first show that d is a common divisor of a and b.

We claim that $d|a$. Suppose not. By Theorem 1.6, we may suppose

$$a = dq + r, 0 < r < d.$$

Then

$$r = a - dq = a - (xaq + ybq) = a(1 - xq) + byq.$$

Therefore, $r \in P$ and it is smaller than d. But d is the smallest element in P. Hence, we conclude that $d \mid a$. In a similar way, we find that $d \mid b$. This shows that d is a common divisor of a and b.

Finally, if $c|a$ and $c|b$ then $a = cu$ and $b = cv$. This implies, by (1.2), that

$$xa + yb = c(ux + vy) = d$$

and hence, $c|d$. This shows that d satisfies Definition 1.9 and we conclude that $d = (a, b)$. □

REMARK 1.14 Note that the above theorem says that if $d = (a, b)$ then there exists integers x and y such that

$$d = ax + by.$$

We now list some basic properties of the greatest common divisor of two integers.

THEOREM 1.15 Let a, b and c be integers. Then

(a) $(a, b) = (b, a)$ (commutative law),
(b) $(a, (b, c)) = ((a, b), c)$ (associative law),
(c) $(ac, bc) = |c|(a, b)$, and
(d) $(a, 1) = (1, a) = 1$. If a is non-zero, then $(a, 0) = (0, a) = |a|$.

Proof
We will prove only (c) and leave the proofs of the other statements as exercises.

Let $d = (ac, bc)$ and $\delta = (a, b)$. Since $d = (ac, bc)$, there exists u, v such that

$$d = acu + bcv = c(au + bv) = |c|\frac{c}{|c|}(au + bv).$$

Since $c/|c| = \pm 1$, we conclude that $|c||d$. Therefore, $d|ac$ implies that $d/|c|$ divides a. Similarly $d/|c|$ divides b. This implies that $d/|c|$ divides $(a, b) = \delta$ and so, $d \leq \delta|c|$.

Next, $\delta|a$ implies that $|c|\delta$ divides $ca(|c|/c)$ or $|c|\delta|ca$ since $|c|/c = \pm 1$. Similarly, $\delta|b$ implies that $|c|\delta$ divides bc. Therefore, $|c|\delta$ divides $(ac, bc) = d$ and so, $d \leq |c|\delta$. Together with $d \leq \delta|c|$ that is established in the previous paragraph, we conclude that $d = \delta|c|$.

□

We recall that two integers a and b are relatively prime (see Definition 1.5) if their only common divisor is 1. Now, (a, b) is a common divisor and this means that $(a, b) = 1$ since there is only one common divisor. In other words, we find that a and b are relatively prime if and only if $(a, b) = 1$.

THEOREM 1.16 Let a and b be integers. Then $(a, b) = 1$ (or a and b are relatively prime) if and only if $1 = ax + by$ for some integers x and y.

Proof
Note that if $(a, b) = 1$, then $1 = ax + by$ for some integers x and y.

Conversely, if $1 = ax + by$, then $(a, b)|a$ and $(a, b)|b$, and therefore $(a, b)|1$. This implies that $(a, b) = 1$. □

EXAMPLE 1.12 Let a, b, c be non-zero integers. Show that if $(a, b) = 1$ and $(a, c) = 1$, then $(a, bc) = 1$.

Solution

Since $(a, b) = 1$ and $(a, c) = 1$,

$$ax + by = 1 \quad \text{and} \quad au + cv = 1$$

for some integers x, y, u, v. Hence,

$$1 = (ax + by)(au + cv) = a(axu + byu + xcv) + bc(yv).$$

Therefore, $(a, bc) = 1$.

EXAMPLE 1.13 Show that if $(m, n) = 1$ then $m|c$ and $n|c$ implies that $(mn)|c$.

Solution

Since $m|c$ and $n|c$, we have $c = mh$ and $c = nk$ for some integers h and k. Now, the fact that $(m, n) = 1$ implies that

$$1 = mu + nv$$

for some integers u and v. Hence,

$$c = mcu + ncv = m(nk)u + n(mh)v = mn(ku + hv).$$

This implies that $(mn)|c$.

EXAMPLE 1.14 Let $d|a$ and $d|b$. Show that $(a, b) = d$ if and only if $(a/d, b/d) = 1$.

Solution

If $d = (a, b)$ then $d = au + bv$ for some integers u and v¿ This implies that $1 = (a/d)u + (b/d)v$ and therefore $1 = (a/d, b/d)$.

Conversely, if $1 = (a/d, b/d)$, then $d = d(a/d, b/d) = (a, b)$.

EXAMPLE 1.15 Suppose $(a, b) = 1$. Show that $(a + b, a^2 + b^2) = 1$ or 2.

Solution

First, recall that $(a,b) = 1$ implies that $(a^2, b^2) = 1$. Let $d = (a+b, a^2+b^2)$. Then $a \equiv -b \pmod{d}$ and $a^2+b^2 \equiv 0 \pmod{d}$. Substituting the first congruence equation into the second one, we observe that

$$0 \equiv a^2 + b^2 \equiv (-b)^2 + b^2 \equiv 2b^2 \pmod{d}.$$

Similarly,

$$0 \equiv a^2 + b^2 \equiv a^2 + (-a)^2 \equiv 2a^2 \pmod{d}.$$

Therefore $d|2a^2$ and $d|2b^2$ which implies that $d|(2a^2, 2b^2)$. Since $(2a^2, 2b^2) = 2(a^2, b^2)$ and that $(a^2, b^2) = 1$, we conclude that $d|2$. Hence, $d = 1$ or 2.

1.4 The Euclidean Algorithm

THEOREM 1.17 (The Euclidean Algorithm) Given positive integers a and b, where $a \nmid b$. Let $r_0 = b, r_1 = a$, and apply the division algorithm repeatedly to obtain a set of remainders $r_2, r_3, ..., r_n, r_{n+1}$ defined successively by the relations

$$\begin{aligned} r_0 &= r_1 q_1 + r_2, & 0 < r_2 < r_1 \\ r_1 &= r_2 q_2 + r_3, & 0 < r_3 < r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} &= r_n q_n + r_{n+1}, & r_{n+1} = 0. \end{aligned}$$

Then r_n, the last nonzero remainder in this process is (a,b), the greatest common divisor of a, and b.

We need a simple lemma.

LEMMA 1.18 Let a, b, q, and r be integers such that $b = aq + r$, then $(a,b) = (a,r)$.

Proof

Let $d = (a,b)$ and $d' = (a,r)$. Note that since $d|a$ and $d|b$, we find that $d|(b-aq)$ by Theorem 1.5 (c). Hence, $d|r$ and d is a common divisor of b and r. By Definition 1.9 (c), $d|d'$ since $d' = (a,r)$. Similarly, $d'|b$ and $d'|r$ implies that $d'|(aq+r)$ by Theorem 1.5 (c) and consequently, $d'|b$. By Definition 1.9 (c), $d'|d$ since $d = (a,b)$. Therefore, by Theorem 1.5 (d), $d = d'$. □

We now complete the proof of Theorem 1.17.

Proof of Theorem 1.17
There is a stage at which $r_{n+1} = 0$ because the r_i are decreasing and nonnegative. Next, applying Lemma 1.18, we find that

$$(a, b) = (r_0, r_1) = (r_1, r_2) = \cdots = (r_n, r_{n+1}) = (r_n, 0) = r_n.$$

This completes the proof of Theorem 1.17. □

EXAMPLE 1.16 Find $(196884, 576)$.

Solution

$$196884 = 341 \cdot 576 + 468$$
$$576 = 1 \cdot 468 + 108$$
$$468 = 4 \cdot 108 + 36$$
$$108 = 3 \cdot 36 + 0.$$

Therefore $(196884, 576) = 36$.

EXAMPLE 1.17 Find integers x and y satisfying

$$43x + 64y = 1.$$

Solution

$$64 = 43 \cdot 1 + 21$$
$$43 = 21 \cdot 2 + 1.$$

Working backwards, we have

$$1 = 43 - 21 \cdot 2 = 43 - 2 \cdot (64 - 43) = 43 \cdot 3 + 64 \cdot (-2).$$

In this section, we define the greatest common divisor of two non-zero integers. The greatest common divisor of k non-zero integers with $k > 2$ can be defined as the number d with the properties that

(a) The integer d is nonnegative.

(b) The integer d is a common divisor of $a_1, a_2, \cdots, a_k$.
(c) If e is any common divisor of $a_1, a_2, \cdots, a_k.$, then $e|d$.

1.5 Least common multiple

DEFINITION 1.11 A *common multiple* of two integers a and b is a positive integer m with the property that $a|m$ and $b|m$.

DEFINITION 1.12 The *least common multiple* of two integers a and b is an integer m such that

(a) $m > 0$,
(b) $a|m$ and $b|m$, and
(c) If c is a common multiple of a and b then $m|c$.

We first establish the existence of the least common multiple of a and b. Consider the set

$$S := \{c \in \mathbf{Z}^+ \mid a|c \text{ and } b|c\}.$$

By the least integer axiom, there exists a common multiple m of a and b such that $m \leq c$ if c is any common multiples of a and b. We need to show that $m|c$. Suppose $m \nmid c$ for some common multiple c of a and b. Write

$$c = mq + r, 0 < r < m.$$

Since $a|c$ and $a|m$, we find that $a|r$. Similarly, $b|r$ and hence $r \in S$. But $r < m$, contradicting the minimality of m. Hence, $m|c$.

We now give two properties of the least common multiple of a and b. Note that part (a) of the following result is an analogue of $(ka, kb) = |k|(a, b)$.

THEOREM 1.19 Let a, b, m be positive integers. Then

(a) $[ma, mb] = m[a, b]$, and
(b) $[a, b] \cdot (a, b) = ab$.

Proof

Let $H = [ma, mb]$ and $h = [a, b]$. Then $a|h$ and $b|h$. Hence, $ma|(mh)$ and $mb|(mh)$. This implies that $H|(mh)$ since H is the least common multiple.

Next, $ma|H$ and $mb|H$. Hence, $a|(H/m)$ and $b|(H/m)$ and so $h|(H/m)$. Hence $mh|H$. Therefore $H = mh$.

To prove (b), we first show that if $(h,k)=1$ then $[h,k]=hk$.

Suppose $(h,k)=1$ and that $h|c$ and $k|c$. Then by Example 1.13, we conclude that $hk|c$. This implies that $hk=[h,k]$ since all common multiples of h and k are divisible by hk.

Now, let a and b be two integers and $d=(a,b)$. Then by (a), $[a,b]=d[a/d,b/d]$. Since $(a/d,b/d)=1$, we conclude that $[a/d,b/d]=ab/d^2$. Therefore $[a,b]=d(ab/d^2)=ab/d$, or $(a,b)[a,b]=ab$. □

1.6 Euclid's Lemma

We know that if $c\neq 0$ then $ca=cb$ implies that $a=b$. This is the law of cancelation for equality. The law is not true in general if we replace "=" by $\equiv$. For example, $15\equiv 3 \pmod{12}$ but $5\not\equiv 1 \pmod{12}$. This shows that the law of cancellation does not hold in general for congruences.

The next result (Euclid's Lemma) shows that the law of cancelation holds if we impose a condition on the integer c.

THEOREM 1.20 If $n|(ca-cb)$ and $(c,n)=1$ then $n|(a-b)$.

Proof
Recall from Theorem 1.13 that if $(c,n)=1$ then there exist integers x and y such that $cx+ny=1$. Multiplying a and b yields

$$acx+any=a$$

and

$$bcx+bny=b,$$

respectively. This implies that

$$(ac-bc)x+n(ay-by)=a-b.$$

Since $n|(ac-bc)$ and $n|n$, we conclude that $n|(a-b)$. Since $ac\equiv bc \pmod{n}$, we conclude that $a-b\equiv(ac-bc)x\equiv 0 \pmod{n}$. □

Theorem 1.20 implies that if $n|cd$ (which implies that $n|(cd-c\cdot 0)$) and $(n,c)=1$ then $n|d$.

The following result of Euclid follows immediately from the above observation.

COROLLARY 1.21 Let p be a prime. If $p|ab$, then $p|a$ or $p|b$.

Proof
For any integer n, $(n,p)=1$ or p since p has only two divisors. Suppose $p\nmid a$. Then (p,a)=1. Therefore $p|ab$ implies that $p|b$. □

By induction, we have the following:

COROLLARY 1.22 Let p be a prime. If $p|(a_1a_2\cdots a_m)$ then $p|a_k$ for some k.

1.7 Fundamental Theorem of Arithmetic

THEOREM 1.23 (Fundamental Theorem of Arithmetic) Every positive integer $n > 1$ can be expressed as a product of primes; this representation is unique apart from the order in which the factors occur.

Proof

We first show that n can be expressed as a prime or a product of primes. We use induction on n. The statement is clearly true for $n = 2$ since 2 is a prime. Suppose m is a prime or a product of primes for $2 \leq m \leq n-1$. If n is a prime then we are done. Suppose n is composite then $n = ab$, where $1 < a, b < n$. By induction each of the a and b is either a prime or a product of primes. Hence, $n = ab$ is a product of primes. By mathematical induction, every positive integer $n > 1$ is a prime or a product of primes.

To prove uniqueness, we use induction on n again. If $n = 2$ then the representation of n as a product of primes is clearly unique. Assume, then that it is true for all integers greater than 1 and less than n. We shall prove that it is also true for n. If n is prime, then there is nothing to prove. Assume, then, that n is composite and that n has two factorizations, say,

$$n = p_1p_2\cdots p_s = q_1q_2\cdots q_t. \tag{1.3}$$

Since p_1 divides the product $q_1q_2\cdots q_t$, it must divide at least one factor. Relabel $q_1, q_2, ..., q_t$ so that $p_1|q_1$. Then $p_1 = q_1$ since both p_1 and q_1 are primes. In (1.3), we may cancel p_1 on both sides to obtain

$$n/p_1 = p_2\cdots p_s = q_2\cdots q_t.$$

Now the induction hypothesis implies that the two factorizations of n/p_1 must be the same, apart from the order of the factors. Therefore, $s = t$ and the factorizations in (1.3) are also identical, apart from order. This completes the proof. □

EXAMPLE 1.18 Let

$$a = \prod_p p^{\alpha_p} \quad \text{and} \quad b = \prod_p p^{\beta_p}.$$

Show that

$$(a,b) = \prod_p p^{\min(\alpha_p,\beta_p)} \quad \text{and} \quad [a,b] = \prod_p p^{\max(\alpha_p,\beta_p)}.$$

Solution

We show the first equality. Let

$$d = \prod_p p^{\min(\alpha_p,\beta_p)}.$$

Note first that for nonnegative integers u and v, $u \leq v$ if and only if $n^u | n^v$ for any positive integer n. Since $\min(\alpha_p, \beta_p) \leq \alpha_p$ for each prime p, we conclude that $d|a$. Similarly, $d|b$. Hence, d is a common divisor of a and b.

Next, suppose $c|a$ and $c|b$. Write

$$c = \prod_p p^{\gamma_p}.$$

By the observation in the beginning of the first paragraph, we conclude that $\gamma_p \leq \alpha_p$ and $\gamma_p \leq \beta_p$. Hence $\gamma_p \leq \min(\alpha_p, \beta_p)$ and hence $c|d$. This implies that d is the greatest common divisor of a and b.

The proof of the second assertion is similar and is left as exercise.

REMARK 1.24 Since $\min(\alpha,\beta) + \max(\alpha,\beta) = \alpha + \beta$ for any integers α and β, we conclude that

$$(a,b)[a,b] = ab.$$

1.8 Euclid's Lemma and the linear Diophantine equation

In Example 1.17, we give a particular solution to

$$43x + 64y = 1.$$

In general, an equation of the type

$$ax + by = m$$

is called a linear Diophantine equation. We now discuss how one can obtain general solutions of linear Diophantine equation.

Suppose $(a,b) = d$. If $d \nmid m$ then the equation has no solution. Suppose $d|m$. Let x_0 and y_0 be a particular solution of $ax + by = m$. Let X and Y be general solution of the equation. Then

$$a(X - x_0) = b(y_0 - Y).$$

Hence,

$$\frac{a}{d}(X - x_0) = \frac{b}{d}(y_0 - Y).$$

Since $(a/d, b/d) = 1$, we conclude from Theorem 1.20 that

$$y_0 - Y = \frac{a}{d}k \quad \text{and} \quad X - x_0 = \frac{b}{d}k.$$

The general solution is therefore

$$X = \frac{b}{d}k + x_0 \quad \text{and} \quad Y = -\frac{a}{d}k + y_0.$$

EXAMPLE 1.19 There are 3 castaways and a monkey on a desert island who have gathered a pile of coconuts which are to be divided the next day. During the night one man arises, divides the pile into 3 equal parts, and finds one coconut left over, which he gives to the monkey. He then hides his share away from the pile. Each of the 3 men repeats the performance. The last man leaves a pile which is exactly divisible by 3. What was the minimum number of coconuts in the original pile?

Solution

Let N be the number of coconuts. Then we know from the three nights that $N = 3a + 1, 2a = 3b + 1, 2b = 2c + 1, 2c = 3d$. This yields $8N = 81d + 38$. The general solution for this equation is $N = 81k - 380$. The smallest k for which N is positive is $k = 5$ or $N = 25$.

1.9 Linear Congruence equation

A linear congruence equation is an equation of the form

$$ax \equiv b \pmod{n}.$$

In this section, we will prove that

THEOREM 1.25 Let $a, b > 0$ be integers and $d = (a, b)$. Suppose $d|N$. Then the linear congruence

$$ax \equiv N \pmod{b} \tag{1.4}$$

has d mutually incongruent solutions modulo b.

Proof
Suppose $ax \equiv N \pmod{b}$. Then

$$ax = N - by. \tag{1.5}$$

If x_0 and y_0 are integers satisfying (1.5), then the general solution of (1.5) is

$$X = \frac{b}{d}k + x_0 \quad \text{and} \quad Y = -\frac{a}{d}k + y_0.$$

This implies that X is a solution of (1.4) for any integer k. We claim that modulo b there are exactly d solutions. For any integer k, let $k = dq + r$ with $0 \leq r < d$. Then

$$x_0 + \frac{b}{d}(dq + r) \equiv x_0 + \frac{b}{d}r \pmod{b}.$$

Therefore, any solution of (1.4) must belong to the set

$$S = \left\{ \frac{b}{d}k + x_0, 0 \leq k < d \right\}.$$

We now show that the solutions in S are incongruent modulo b. Suppose

$$x_0 + \frac{b}{d}i \equiv x_0 + \frac{b}{d}j \pmod{b}.$$

Then

$$\frac{b}{d}(i - j) \equiv 0 \pmod{b}.$$

This implies that $d|(i-j)$. Since i and j are both less than d, $i = j$. Hence there are exactly d solutions to (1.4). □

REMARK 1.26 Theorem 1.25 will be needed for determining the number of solutions of congruences of the type

$$x^m \equiv c \pmod{n}.$$

We end this section by proving Wilson's Theorem using solutions of linear congruence equations.

THEOREM 1.27 Let p be an odd prime. Then

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof
For $1 \leq a \leq p-1$, we consider the equation

$$ax \equiv 1 \pmod{p},$$

which has exactly one solution modulo p by Theorem 1.25. If $a = 1$, then $x = 1$ and if $a = p - 1$, $x = p - 1$. If $a \neq 1, p - 1$, then the solution $x \neq a$. In other words, we can regroup the integers from 1 to $p - 1$ in the form

$$\{1, p - 1\} \cup S$$

where

$$S = \bigcup_{a=2}^{p-2} \{a\}.$$

The integers from S can be paired up as (a', b') so that $a'b' \equiv 1 \pmod{p}$. This implies that

$$(p-1)! \equiv 1 \cdot (p-1) \cdot \prod_{\substack{2 \leq a', b' \leq p-2 \\ a'b' \equiv 1 \pmod{p}}} a'b' \equiv -1 \pmod{p}.$$

This completes the proof of Wilson's Theorem. □

EXAMPLE 1.20 Show that if n is composite, then $(n-1)! \not\equiv -1 \pmod{n}$.

Solution

Since n is composite, there exists an integer d with $1 < d < n$ such that $d|n$. Since $d|(n-1)!$, $(n-1)! \equiv 0 \pmod{d}$. Suppose $(n-1)! \equiv -1 \pmod{n}$, then $(n-1)! \equiv -1 \pmod{d}$ and this contradicts the previous observation that $d|(n-1)!$.

REMARK 1.28 Let $M(n) = (\mathbf{Z}/n\mathbf{Z})^*$ be the subset of $\mathbf{Z}/n\mathbf{Z}$ that contains $[r]_n$ such that $(r, n) = 1$. This set forms a group under the binary operation

$$[a]_n \bullet [b]_n = [ab]_n.$$

Since $M(n)$ is a group, each $[a]_p \in M(p)$ has a unique inverse. Only $[1]_p$ and $[p-1]_p$ have inverses that are identical to itself. For other element $[a]_p \in M(p)$, its inverse $[a]_n^{-1}$ is distinct from $[a]_p$. Therefore.

$$[1]_p \bullet [2]_p \bullet \cdots \bullet [p-1]_p = [-1]_p,$$

and this completes the proof of Wilson's Theorem.

REMARK 1.29 Wilson's Theorem can be used to design a primality test, namely, an algorithm for determining whether an input number is prime. But this algorithm is extremely inefficient. A primality test with "polynomial time" was discovered in 2004 by M. Agarwal, N. Kayal and N. Saxena.

1.10 Wilson's Theorem and primes of the form $x^2 + y^2$

LEMMA 1.30 Let $p \equiv 1 \pmod 4$ be a prime. Then there exists an integer u such that

$$u^2 \equiv -1 \pmod p.$$

Proof
Write $p - a = -a \pmod p$. Then $(p-1)! \equiv -1 \pmod p$ can be rewritten as

$$(-1)^{(p-1)/2} \left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod p.$$

The integer

$$u = \left[\left(\frac{p-1}{2}\right)!\right]^2$$

satisfies

$$u^2 \equiv -1 \pmod p.$$

□

THEOREM 1.31 If $p \equiv 1 \pmod 4$ is a prime then it is a sum of two squares.

Proof
Suppose $p \equiv 1 \pmod 4$ then from Lemma 1.30, there exists u such that

$$u^2 \equiv -1 \pmod p. \tag{1.6}$$

We may choose u to be an integer such that $|u| \leq \dfrac{p-1}{2}$ and write (1.6) as

$$u^2 + 1 = kp \tag{1.7}$$

for some positive integer k. Let

$$S := \{m | x^2 + y^2 = mp, \quad m \in \mathbf{Z} \text{ with } 1 \leq m < p.\}$$

Note that by (1.7), we have $u^2 + 1 = kp$. Furthermore, $|u| \leq \dfrac{p-1}{2}$ implies that $u^2 + 1 < p^2$ and so $1 \leq k < p$. Hence, $k \in S$ and S is non-empty.

By the least integer axiom, S contains a minimal positive m_0 satisfying the conditions. If $m_0 = 1$ then we are done.

Suppose $m_0 > 1$ and that $m_0 p = x_0^2 + y_0^2$. If $m_0 | x_0$ and $m_0 | y$ then $m_0^2 | (x_0^2 + y_0^2)$

or $m_0^2 | m_0 p$. This implies that $m_0 | p$, which is impossible since $m_0 < p$. Hence $m_0 \nmid x_0$ or $m_0 \nmid y_0$. Let

$$x_1 = x_0 - m_0 r, y_1 = y_0 - m_0 s$$

where $|x_1| < m_0/2$ and $|y_1| < m_0/2$. Note that since $m_0 \nmid x_0$ or $m_0 \nmid y_0$, $x_1^2 + y_1^2 > 0$. Now,

$$0 < x_1^2 + y_1^2 \leq m_0^2/2 < m_0^2.$$

Hence,

$$x_1^2 + y_1^2 = m_1 m_0$$

with $m_1 < m_0$.

Next,

$$m_0^2 m_1 p = (x_0^2 + y_0^2)(x_1^2 + y_1^2) = (x_0 x_1 + y_0 y_1)^2 + (x_0 y_1 - x_1 y_0)^2.$$

Now, observe that

$$X = x_0 x_1 + y_0 y_1 = x_0(x_0 - m_0 r) + y_0(y_0 - m_0 s) = m_0 w,$$

for some integer w. Similarly,

$$Y = x_0 y_1 - x_1 y_0 = m_0 v.$$

Therefore,

$$m_0^2 m_1 p = X^2 + Y^2 = m_0^2(w^2 + v^2).$$

This implies that

$$w^2 + v^2 = m_1 p. \tag{1.8}$$

Therefore $m_1 \in S$. Since $m_1 < m_0$, this contradicts the minimality of m_0 in S. This implies that $m_0 = 1$ in the first place and we are done. □

1.11 Appendix : The cyclic group $(\mathbf{Z}, +)$ and the greatest common divisor

Let G be a nonempty set and $*$ be function from $G \times G$ to G satisfying

(a) There exists an $e \in G$ such that for all $g \in G$, $e * g = g * e = g$.
(b) For all $g \in G$, there exists a $g' \in G$ such that $g * g' = g' * g = e$.
(c) For all $g, h, k \in G$, $g * (h * k) = (g * h) * k$.

The set G together with the *binary operation* $*$ is called a group.

If H is a nonempty subset of G and $(H, *)$ is a group, we say that H is a subgroup of G and the notation is $H \leq G$. One can use a simple criterion to check if H were a subgroup of G. This is given by $H \leq G$ if and only if for all $h, k \in H$, $hk^{-1} \in H$.

The simplest example of a group is perhaps $(\mathbf{Z}, +)$. The identity is 0 and the inverse of n is $-n$. This is a cyclic group (that is, a group that is generated by one element, namely 1). Using Division Algorithm, we can show that any subgroup of a cyclic group is cyclic.

Now, if we define

$$T = \{au + bv | u, v \in \mathbf{Z}\},$$

then we can, using the subgroup criterion, check that T is a subgroup of $\mathbf{Z}$ since $au+bv-(au'+bv') = a(u-u')+b(v-v') \in T$. Since $(\mathbf{Z}, +)$ is cyclic, we conclude that T is cyclic and hence $T = d\mathbf{Z}$, that is, T is generated by one element d. We may choose d to be positive. Now, note that both $a = a + 0 \cdot b$ and $b = a \cdot 0 + b$ are in T. Hence $d|a$ and $d|b$. Since $d \in T$, $d = au + bv$ for some integers u, v. Suppose $c|a$ and $c|b$. Then from the representation of d, we conclude that $c|d$. Hence d is the greatest common divisor of a and b.

2 Fermat's Little Theorem and Euler's Theorem

2.1 Fermat's Little Theorem

DEFINITION 2.1 If $x \equiv y \pmod{m}$, then y is called a residue of x modulo m. A set $x_1, x_2, \cdots, x_m$ is called a complete system of residues modulo m if for every integer y there is one and only one x_j such that $y \equiv x_j \pmod{m}$.

The complete system of residues modulo m is not unique. For example, when $n = 5$, the set $\{0, 1, 2, 3, 4\}$ is a complete system of residues modulo 5. The set $\{5, 11, 22, 33, 14\}$ is also a complete system of residues modulo 5. Note that the set $\{1, 11, 12, 13, 14\}$ is not a complete system of residues modulo 5 since $1 \equiv 11 \pmod{5}$.

DEFINITION 2.2 For a positive integer n, the set $\{0, 1, 2, \cdots n-1\}$ is called the least non-negative residues modulo n.

THEOREM 2.1 (Fermat's Little Theorem) If p is a prime and $p \nmid a$ then

$$a^{p-1} \equiv 1 \pmod{p}.$$

REMARK 2.2 Fermat's Little Theorem is sometimes written as: For a fixed prime p,

$$a^p \equiv a \pmod{p}$$

for all integer a. Note that when written in this form, the condition $p \nmid a$ can be removed since $a^p \equiv a \equiv 0 \pmod{p}$ when $p|a$.

Proof
Let

$$S = \{0, 1, 2, \cdots, p-1\}.$$

Suppose $(a,p)=1$ or $p\nmid a$. Let $T=\{a\cdot 0, a\cdot 1,\cdots, a\cdot(p-1)\}$. Note that no two elements in T are congruent to each other modulo p. For if $ka\equiv ja \pmod p$, then $k\equiv j \pmod p$, since $(a,p)=1$ and cancelation law applies. Hence, T is a complete set of residues modulo p. Hence, the product of all nonzero elements in T must be congruent to the product of all nonzero elements in S. In other words, if we multiply all the elements in $T-\{0\}$, the product must be congruent modulo p to the product of all the elements in $S-\{0\}$. Therefore,

$$a^{p-1}(p-1)!\equiv (p-1)! \pmod p.$$

Since $p\nmid (p-1)!$, $(p,(p-1)!)=1$ and cancelation law holds again. Therefore, $a^{p-1}\equiv 1 \pmod p$. □

Fermat's Little Theorem can be a labor-saving device in certain calculations.

EXAMPLE 2.1 Prove that $1835^{1910}+1986^{2061}\equiv 0 \pmod 7$.

Solution

We have $1835\equiv 1 \pmod 7$ and $1986\equiv 5 \pmod 7$. Therefore

$$1835^{1910}+1986^{2061}\equiv 1+5^{2061} \pmod 7.$$

Now, $2061\equiv 3 \pmod 6$ and therefore, $2061=6q+3$, for some integer q. Hence,

$$5^{2061}\equiv 5^{6q+3}\equiv (5^6)^q\cdot 5^3\equiv 5^3 \pmod 7$$

since $5^6\equiv 1 \pmod 7$, by Theorem 1.1. The congruence thus reduces to

$$1+5^{2061}\equiv 1+5^3\equiv 1+6\equiv 0 \pmod 7.$$

Fermat's Little Theorem may also be used as a tool for primality testing. For example, for a given n if we can find an a such that $(a,n)=1$ and $a^{n-1}\not\equiv 1 \pmod n$ then we conclude immediately that a is not relatively prime to n. This implies that n is not a prime. The following example illustrate this point.

EXAMPLE 2.2 Show that 57 is not a prime using Fermat's Little Theorem.

Solution

We have

$$2^{57}\equiv 2^7\cdot 2^{10\cdot 5}\equiv 2^7\cdot(-2)^5\equiv -2^2\cdot 2^{10}\equiv 8 \pmod{57}.$$

Since $2^{57}\not\equiv 2 \pmod{57}$, 57 is composite.

Of course this test is very inefficient for several reasons. Firstly, one might

need to select a number a several times before arriving at a conclusion that n is composite. Secondly, computing powers of a number is very time consuming. Thirdly, it may be inconclusive even if $a^{n-1} \equiv 1 \pmod{n}$ for all $a < n$ as the following example shows.

EXAMPLE 2.3 Show that $a^{561} \equiv a \pmod{561}$ for $a < 561$.

Solution

If a is prime to 561, then $a^2 \equiv 1 \pmod{3}$, $a^{10} \equiv 1 \pmod{11}$ and $a^{16} \equiv 1 \pmod{17}$. Now,

$$\begin{aligned} a^{560} &\equiv (a^2)^{280} \equiv 1 \pmod{3} \\ a^{560} &\equiv (a^{10})^{56} \equiv 1 \pmod{11} \\ a^{560} &\equiv (a^{16})^{35} \equiv 1 \pmod{17} \end{aligned}$$

Therefore $a^{560} \equiv 1 \pmod{561}$, or $a^{561} \equiv a \pmod{561}$. If a is not relatively prime to 561, the above still holds. For if $N = 3 \cdot 11 \cdot 17$ and $(a, 561) = 561$, then

$$a^{561} \equiv a \equiv 0 \pmod{561}.$$

If $N = 3, 11, 17, 3 \cdot 11, 3 \cdot 17$, or $11 \cdot 17$ and $(a, 561) = N$, then since N is square free, $(a, 561/N) = 1$ and hence, using Fermat's Little Theorem, we have

$$a^{561} \equiv a \pmod{561/N}.$$

Since $N|a$, we also have

$$a^{561} \equiv a \equiv 0 \pmod{N}.$$

Hence,

$$a^{561} \equiv a \pmod{561}.$$

A number which satisfies the property that $a^n \equiv a \pmod{n}$ for all a is called a Carmichael number. It has been a conjecture for nearly 90 years that there are infinitely many Carmichael numbers. This result has only recently been proved by W.R. Alford, A. Granville, C. Pomerance (see Ann. of Math. 140 (1994), 703-722).

2.2 An extension of Fermat's Little Theorem: The Euler Theorem

Fermat's Little Theorem is false when n is composite. For example, $5^5 \equiv 5 \pmod 6$, i.e., $5^6 \not\equiv 5 \pmod 6$. In this Section we will learn an extension of Fermat's Little Theorem. But first let us define a very important function.

DEFINITION 2.3 The function $\varphi(n)$ is defined to be the number of elements $1 \leq x < n$ which are relatively prime to n. The function $\varphi(n)$ is usually called *Euler's φ function.*

REMARK 2.3 The number $\varphi(n)$ is the number of elements in $M(n)$.

EXAMPLE 2.4 There are altogether 2 numbers less than 6 which are relatively prime to 6. These are 1 and 5. Therefore, $\varphi(6) = 2$. For $n = 12$, $\varphi(12) = 4$ and these four numbers are $1, 5, 7, 11$.

EXAMPLE 2.5 Note that when p is prime, all the numbers $1 \leq x < p$ are relatively prime to p and so,

$$\varphi(p) = p - 1. \tag{2.1}$$

For example, $\varphi(7) = 6$ and the numbers that are relatively prime to 7 are $1, 2, \cdots, 6$.

We are now ready to state Euler's Theorem:

THEOREM 2.4 (Euler's Theorem) Suppose $(a, n) = 1$. Then

$$a^{\varphi(n)} \equiv 1 \pmod n.$$

Note that when n is prime, by (2.1), $\varphi(p) = p - 1$. So Theorem 2.4 reduces to Fermat's Little Theorem, since

$$a^{\varphi(p)} \equiv a^{p-1} \equiv 1 \pmod p.$$

Proof

The idea of the proof is the same as that of Fermat's Little Theorem. Consider the set

$$S := \{a_1, a_2, \cdots, a_{\varphi(n)}\},$$

where S contains all the positive integers $x < n$ which are relatively prime to n. (Note by definition, there are $\varphi(n)$ of them). Suppose a is relatively prime to n. We define

$$T = \{a \cdot a_1, a \cdot a_2, \cdots, a \cdot a_{\varphi(n)}.\}.$$

Once again, no two elements in T are congruent modulo n. For if

$$a \cdot a_i \equiv a \cdot a_j \pmod{n},$$

then

$$a_i \equiv a_j \pmod{n}$$

since $(a, n) = 1$. Hence, following the argument as in the case of the proof of Fermat's Theorem, we conclude that each element in T is congruent modulo n to exactly one element in S and we conclude that

$$a^{\varphi(n)} \prod_{k=1}^{\varphi(n)} a_k \equiv \prod_{k=1}^{\varphi(n)} a_k \pmod{n}.$$

Once again since $(a_i, n) = 1$ we have

$$\left(\prod_{k=1}^{\varphi(n)} a_k, n \right) = 1$$

and applying cancelation law, we obtain

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

□

REMARK 2.5 The Lagrange Theorem states that the order of a subgroup H of G divides the order of G. Let $G = M(n)$ and $[a]_n \in G$. Let H be the cyclic group of G generated by $[a]_n$. Then $H = \{[a]_n^j | 1 \leq j \leq N\}$ where $[a]_n^N = [1]_n$. The order of $[a]_n$ is N. By Lagrange's Theorem, $N||M(n)|$ or $N|\varphi(n)$. This yields $\varphi(n) = Nk$ for some positive integer k. Now $[a]_n^N = [1]_n$ implies that $[a]_n^{\varphi(n)} = ([a]_n^N)^k = [1]_n$ and therefore, Euler's Theorem follows.

EXAMPLE 2.6 Find the remainder of 4444^{4444} when it is divided by 9.

Solution

Observe that $4444 \equiv -2 \pmod 9$ and $\varphi(9) = 6$ (the positive integers < 9 and relatively prime to 9 are $1, 2, 4, 5, 7, 8$). Since $a^6 \equiv 1 \pmod 9$ when $(a, 9) = 1$ by Theorem 2.4. It is natural to write the exponent in form $6q+r$. Now, $4444 = 6q+4$ and so,

$$4444^{4444} \equiv (-2)^{6q+4} \equiv ((-2)^6)^q \cdot (-2)^4 \equiv (-2)^4 \equiv 7 \pmod 9.$$

Hence, the remainder is 7.

REMARK 2.6 The above example is the final step in the solution of Problem 4 of IMO 1975.

EXAMPLE 2.7 Find the last two digits of 9^{9^9}.

Solution

Since $\varphi(100) = 40$, $9^{40} \equiv 1 \pmod{100}$. Next, $9^9 = 387420489 = 40 \times 9685512 + 9$. Therefore $9^{9^9} \equiv 9^9 \pmod{100}$. But we have seen that $9^9 = 387420489$ and so the last two digits of 9^{9^9} are 89.

REMARK 2.7 Euler's Theorem can be used to solve Linear congruences such as

$$ax \equiv c \pmod m$$

when $(a, m) = 1$. One simply multiplies $a^{\varphi(m)-1}$ to both sides of the congruence to obtain

$$a^{\varphi(m)}x \equiv a^{\varphi(m)-1}c \pmod m.$$

2.3 Finite groups and Euler's Theorem

The division algorithm states that if n is a fixed positive integer then any integer N can be written in the form $qn + r$ where $0 \le r < n$. In other words, the set $\mathbf{Z}$ can be partitioned into n distinct sets, denoted by $[r]_n$, $0 \le r < n$, where

$$[r]_n := \{k \in \mathbf{Z} | k \equiv r \pmod n\}.$$

Let

$$\mathbf{Z}/n\mathbf{Z} = \{[r]_n | 0 \le r < n\}$$

and define the binary operation

$$[a]_n + [b]_n = [a + b]_n.$$

Then the set $\mathbf{Z}/n\mathbf{Z}$ forms a group under the operation $+$. This group is "similar" to the additive group $(\mathbf{Z}, +)$. Of course, the set $\mathbf{Z}$ together with the binary operation $\cdot$ is not a group. Can we construct a group for $\mathbf{Z}/n\mathbf{Z}$ with operation the analogue of $\cdot$? The answer is yes but with a "twist".

We let

$$(\mathbf{Z}/n\mathbf{Z})^* = \{[r]_n | (r, n) = 1, 0 \leq r < n\}.$$

Define

$$[a]_n \cdot [b]_n = [a \cdot b]_n.$$

Then the set $(\mathbf{Z}/n\mathbf{Z})^*$ together with $\cdot$ is a multiplicative group.

The Lagrange Theorem states that for any finite group G, the order of any subgroup H of G divides the order of the group G. To see this, we first construct

$$G/H := \{gH | g \in G\}$$

where the *coset* gH is defined by

$$gH = \{gh | h \in H\}.$$

Note first that if $G = H$, then there is one element in G/H.

If $G \neq H$ and $gH, g'H \in G/H$, we note that

$$gH \cap g'H = \phi.$$

For otherwise, if $x \in gH \cap g'H$, then $x = gh = g'h'$, or $g^{-1}g' \in H$ and $g'H \subset gH$. Similarly, $gH \subset g'H$ and we have $gH = g'H$. Since gH and $g'H$ are disjoint for distinct cosets, we conclude that there are finitely many distinct sets gH in G/H. Furthermore, each $g \in G$ must be in one of these cosets. This implies that

$$G = \cup_{j=1}^{k} g_j H.$$

Using the map

$$\varphi : H \to gH,$$

we find that

$$|H| = |gH|.$$

Therefore,

$$|G| = \sum_{j=1}^{k} |gH| = k|H|.$$

Hence, $|H| \mid |G|$ and this is Lagrange's Theorem for subgroups of finite groups.

Now, one can see that for any element $g \in G$, the set

$$H = \{g^m | m \in \mathbf{Z}\}$$

forms a finite group of order d, where d is the least positive integer such that $g^d = 1$. This positive integer is called the *order of* g in G. Since H is a subgroup of G with $|H| = d$, by Lagrange's Theorem, $d \mid |G|$, or $|G| = d\ell$ for some

positive integer ℓ. Now, $g^d = 1$, where 1 is the identity of the group G. Hence $g^{|G|} = (g^d)^\ell = 1$. We have thus shown that

$$g^{|G|} = 1$$

for all $g \in G$. Applying this to our group $(\mathbf{Z}/n\mathbf{Z})^*$, we find that for any integer a such that $(a, n) = 1$,

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

since $\varphi(n)$ is the number of elements of $(\mathbf{Z}/n\mathbf{Z})^*$.

REMARK 2.8 Let $G = (\mathbf{Z}/n\mathbf{Z})^*$. The elementary proof of Euler's Theorem follows from the fact that the multiplication of a fixed element g of G induces a permutation of the elements in G. In other words, if we define a map

$$\xi : G \to G$$

by $\xi(g_1) = g \cdot g_1$, then ξ is a bijection of G.

EXAMPLE 2.8 Let G be a finite group and k be the order g where $g \in G$. If $g^m = 1_G$ then $k|m$.

Solution

If $k \nmid m$ then $m = kq + r, 0 < r < k$. This implies that

$$1_G = g^m = g^{kq} g^r = g^r$$

and this contradicts the minimality of k.

EXAMPLE 2.9 Let $a > 1$ and $n > 1$ be positive integers. Then $n|\varphi(a^n - 1)$.

Solution

Note that the order of $[a]_{a^n-1}$ in $(\mathbf{Z}/(a^n - 1)\mathbf{Z})^*$ is n. This is because if $0 < d < n$ is the order of $[a]_{a^n-1}$ in $(\mathbf{Z}/(a^n - 1)\mathbf{Z})^*$ then $a^n - 1$ would divide $a^d - 1$, which is impossible. Since $a^{\varphi(a^n-1)} \equiv 1 \pmod{a^n - 1}$ we conclude that $n|\varphi(a^n - 1)$ by the previous example.

2.4 The Chinese Remainder Theorem and solving linear congruence equations

THEOREM 2.9 Let m and n be such that $(m, n) = 1$. Let

$$A(t) = \mathbf{Z}/t\mathbf{Z}.$$

Then the map

$$\xi : A(mn) \to A(m) \times A(n)$$

defined by

$$\xi([k]_{mn}) = ([k]_m, [k]_n)$$

is a bijection.

Proof

First, note that ξ is a well defined map. For, if $[j]_{mn} = [k]_{mn}$ then $\xi([j]_{mn}) = ([j]_m, [j]_n)$. But $j \equiv k \pmod{mn}$ implies that $j \equiv k \pmod{m}$ and $j \equiv k \pmod{n}$. In other words, $\xi([j]_{mn}) = ([k]_m, [k]_n)$ and the map is well defined.

Note that the number of elements in $A(mn)$ and $A(m) \times A(n)$ are equal. It suffices to show that ξ is an injection. Suppose

$$([\ell]_m, [\ell]_n) = ([k]_m, [k]_n).$$

Then $m|(\ell - k)$ and $n|(\ell - k)$. This implies, by Example 1.13 that $mn|(\ell - k)$ since $(m, n) = 1$. Hence, $[\ell]_{mn} = [k]_{mn}$ and the map ξ is injective and hence the map ξ is a bijection. □

Theorem 2.9 is known as the Chinese Remainder Theorem. It says that given integers m and n such that $(m, n) = 1$, the simultaneous congruence equations

$$x \equiv h \pmod{m} \quad \text{and} \quad x \equiv k \pmod{n} \tag{2.2}$$

can be solved. In other words, there exist an integer x satisfying (2.2).

The Chinese Remainder Theorem can be extended to more than two positive integers m and n. More precisely, we can show that if $m_1, m_2, \cdots, m_s$ are pairwise relatively prime, then the system of equations

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_s \pmod{m_s} \end{aligned}$$

is solvable.

The usual way to prove the Chinese Remainder Theorem is by constructing an x that is the solution of

$$x \equiv a \pmod{m} \quad \text{and} \quad x \equiv b \pmod{n}.$$

To do so, one sets

$$x = nta + msb,$$

where $ms \equiv 1 \pmod{n}$ and $nt \equiv 1 \pmod{m}$. Note that with this choice of x,

$$x \equiv nta + msb \equiv nta \equiv a \pmod{m}$$

since $nt \equiv 1 \pmod{m}$. Similarly, we find that

$$x \equiv msb \equiv b \pmod{n}.$$

The only difficulty now is to determine the value s and t that satisfy

$$ms \equiv 1 \pmod{n} \quad \text{and} \quad nt \equiv 1 \pmod{m}.$$

This amounts to solving linear congruence of the form

$$aX \equiv 1 \pmod{k}. \tag{2.3}$$

Note that this linear congruence is solvable only if $(a, k) = 1$. In this case, there exists u and v such that

$$1 = au + kv.$$

Hence $X = u$ is a solution to the linear congruence (2.3).

EXAMPLE 2.10 Find the least positive integer x such that $x \equiv 2 \pmod{3}, x \equiv 3 \pmod{5}$ and $x \equiv 2 \pmod{7}$. Answer: 23.

Solution

Let N be an integer satisfying the congruences. Then $N \equiv 2 \pmod{21}$ and $N \equiv 3 \pmod{5}$. Since $5 \cdot (-4) \equiv 1 \pmod{21}$ and $21 \cdot 1 \equiv 1 \pmod{5}$, we conclude that

$$N = 21 \cdot 3 + (-20) \cdot 2 = 63 - 40 = 23$$

is a solution to the congruences.

2.5 Euler's φ-function

In this section, we establish an important property of $\varphi(n)$ which allows us to compute $\varphi(n)$ if we know the prime factorization of n.

THEOREM 2.10 For positive integers m and n such that $(m, n) = 1$,

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Let

$$M(t) := (\mathbf{Z}/t\mathbf{Z})^* .$$

Note that $|M(t)| = \varphi(t)$. Consider the map

$$\psi : M(mn) \to M(m) \times M(n)$$

defined by

$$\psi([k]_{mn}) = ([k]_m, [k]_n).$$

Note that $\psi = \xi\big|_{M(mn)}$. From the proof of Theorem 2.9, we see that given $([u]_m, [v]_n) \in M(m) \times M(n)$, there exists $[h]_{mn} \in A(mn)$ such that

$$\xi([h]_{mn}) = ([u]_m, [v]_n).$$

We need to show that $[h]_{mn} \in M(mn)$. This follows from the fact that if $[h]_m \in M(m)$ and $[h]_n \in M(n)$, then $[h]_{mn} \in M(mn)$. In other words, if $(h, m) = 1$ and $(h, n) = 1$ then $(h, mn) = 1$. This proves that the map is surjective. Now the map ψ is injective because ξ is injective. We therefore conclude that ψ is a bijection and

$$\varphi(mn) = \varphi(m)\varphi(n).$$

COROLLARY 2.11 Let $n = \prod_p p^{\alpha_p}$. Then

$$\varphi(n) = \prod_p \varphi(p^{\alpha_p}) = \prod_p \left(p^{\alpha_p} - p^{\alpha_p - 1}\right).$$

Proof
We have seen that if $n = p$ is a prime, then $\varphi(p) = p - 1$. If $\alpha_p > 1$, then the integers $p, 2p, \ldots, p^{\alpha_p - 1}p$ are the positive integers less than p^{α_p} which are not relatively prime to p^{α_p}. Hence, $\varphi(p^{\alpha_p}) = p^{\alpha_p} - p^{\alpha_p - 1}$. □

EXAMPLE 2.11 Show that if $d|n$ then $\varphi(d)|\varphi(n)$.

Solution

If $n = 1$ and $d = 1$, the result is true. Observe that the map

$$\vartheta : (\mathbf{Z}/n\mathbf{Z})^* \to (\mathbf{Z}/d\mathbf{Z})^*$$

defined by $\vartheta([a]_n = [a]_d$ is a surjective group homomorphism. By first isomorphism theorem,

$$|\ker \vartheta| = |(\mathbf{Z}/n\mathbf{Z})^*|/|(\mathbf{Z}/d\mathbf{Z})^*|.$$

Therefore, $\varphi(d)|\varphi(n)$.

Alternatively, let

$$n = \prod_p p^{\alpha_p}$$

and

$$d = \prod_p p^{\gamma_p}.$$

Note that in this representation, α_p is non-zero for finitely many p. Now,

$$\varphi(p^{\gamma_p}) = \begin{cases} 1 & \text{if } \gamma_p = 0, \\ p^{\gamma_p - 1}(p-1) & \text{if } \gamma_p > 0. \end{cases}$$

Hence $\varphi(p^{\gamma_p}) | \varphi(p^{\alpha_p})$ for all primes p since $\gamma_p \leq \alpha_p$. Therefore, $\varphi(d) | \varphi(n)$.

EXAMPLE 2.12 Find all integers n such that $\varphi(n) = 10$.

Solution

Let $p|n$. Then $\varphi(p) = p - 1$ must divide $\varphi(n) = 10$. This means that $p - 1 = 1, 2, 5, 10$ and that $p = 2, 3, 11$. Since $\varphi(11) = 10$ and 11 is the only prime that contributes a factor of 5 to $\varphi(n)$, we conclude that $11|n$. Next, if $3|n$ then $\varphi(3) = 2$ and together with $\varphi(11)$ we conclude that the left hand side is greater or equal to 20, which is certainly greater than 10. Therefore, $3 \nmid n$. Hence, $n = 2^a 11$. This implies that $\varphi(n) = \varphi(2^a)10$ and therefore, $a = 0$ or 1. The only solutions to the equation $\varphi(n) = 10$ are 11 and 22.

2.6 An Application to Cryptography

The purpose of studying Cryptography is to protect information transmitted through public communication networks. In the language of cryptography, the information to be concealed is called plaintext. The message in secret form is called ciphertext. To convert plaintext to ciphertext is to encrypt a message and to perform the reverse process is to decrypt a message.

In 1977, R. Rivest, A. Shamir and L. Adleman proposed a public key cryptosystem, which uses only elementary ideas from Number Theory. The enciphering system is now called RSA. Its security depends on the assumption that in the current state of computer technology, the factorization of composite numbers with large prime factors is prohibitively time-consuming.

Each user of RSA system chooses a pair of distinct primes p, q large enough so that the factorization of $n = pq$ (enciphering modulus) is beyond the current computational capabilities. For example one may select p and q with 200 digits and n would have 400 digits. Having selected n, the user then chooses a random positive integer k such that $(k, \varphi(n)) = 1$. The pair (n, k) is placed in a public

file, as user's personal encryption key. This will allow anyone else to encrypt and send a message to that individual. Note that while n is openly revealed the listed public key does not mention the factors p and q of n.

The encryption begins with the conversion of the message into digital alphabets. For example,

$$A = 00, B = 01, \cdots Z = 25, Space = 26.$$

Under this scheme, the message "The brown fox is quick" is transformed into

$$M = 19070426011714221326051423260818261620080210.$$

We assume that $M < n$. If $M > n$ we can break M into blocks of digits $M_1, M_2, \cdots, M_r$, $M_i < n$. To encrypt, raised M to k^{th} power $\pmod n$, i.e.,

$$M^k \equiv r \pmod n$$

and send r.

To decrypt, first recall that k is chosen such that $(k, \varphi(n)) = 1$. Therefore there exist j such that

$$kj \equiv 1 \pmod{\varphi(n)}.$$

This implies that

$$r^j \equiv M^{jk} \equiv M^{\varphi(n)\cdot m+1} \pmod n.$$

If M is coprime to n, then

$$M^{\varphi(n)} \equiv 1 \pmod n.$$

Therefore

$$r^j \equiv M \pmod n,$$

and we retrieve the message. Note that the number j, called the recovery exponent, can only be calculated by someone who knows $\varphi(n) = (p-1)(q-1)$. Therefore, j is secure from an illegitimate third party whose knowledge is limited to the public key (n, k).

We have assumed above that M is relatively prime to n. Suppose M is not relatively prime to $n = pq$. Then $(M, pq) = p$, q, or pq. If the is pq then since $M < pq$, $M = 0$. Suppose without loss of generality that $(M, pq) = p$. Then

$$kj \equiv 1 \pmod{\varphi(n)}$$

implies that

$$kj \equiv 1 \pmod{q-1},$$

$$r^j \equiv M^{kj} \equiv M \pmod q$$

and

$$0 \equiv M^{kj} \equiv M \pmod p.$$

Hence,

$$r^j \equiv M \pmod{pq}$$

and we retrieve the message.

EXAMPLE 2.13 Let $p = 37, q = 73, pq = 2701$. Note that

$$\varphi(n) = 2592.$$

Take $k = 47$. Then $j = 1103$ since $1103 \cdot 47 \equiv 1 \pmod{2592}$. To encrypt the message "No Way Today", we have

$$M = 1314262200242619140300 24.$$

We divide M into blocks of 4:

$$1314 \quad 2622 \quad 0024 \quad 2619 \quad 1403 \quad 0024.$$

Raised to the power of 47 modulo 2592, we have

$$1241 \quad 1848 \quad 0873 \quad 1614 \quad 2081 \quad 0873.$$

This is the ciphertext. Note that to retrieve the message, we only need to raise the numbers in each block to the power 1103 modulo 2701. For example, $1241^{1103} \equiv 1314 \pmod{2701}$.

2.7 Appendix : Group Action and Fermat's Little Theorem

DEFINITION 2.4 If X is a set and G is a group, then G acts on X if there exists a function $\bullet : G \times X \to X$, called an action such that

(i) for $g, h \in G$ and $x \in X$, $\bullet(g, \bullet(h, x) = \bullet(gh, x)$.
(ii) $\bullet(1_G, x) = x$.

Instead of writing $\bullet(g, x)$, we will use $g \bullet x$ to denote the image of (g, x) under $\bullet$.

DEFINITION 2.5 If G acts on a set X, then the *orbit* of x ($x \in X$), denoted by $\mathcal{O}(x)$, is the subset of X given by

$$\mathcal{O}(x) = \{g \bullet x\}.$$

The *stabilizer* of x, denoted by G_x, is the subgroup of G given by

$$G_x = \{g \in G | g_\bullet x = x\}.$$

We recall the following Theorems:

THEOREM 2.12 If G acts on X, then X is a disjoint union of the orbits. If X is finite, then $|X| = \sum_i |\mathcal{O}_{x_i}|$, where one x_i is chosen from each orbits.

Proof
We need to show that if $\mathcal{O}_x \cap \mathcal{O}_y \neq \phi$, then $O_x = O_y$. Let $z \in \mathcal{O}_x \cap \mathcal{O}_y$. Then $z = g_\bullet x = g'_\bullet y$. This implies that $x = g^{-1}g'_\bullet y$ and so $\mathcal{O}_x \subset \mathcal{O}_y$. Similarly, $\mathcal{O}_y \subset \mathcal{O}_x$ and hence, $\mathcal{O}_x = \mathcal{O}_y$. □

THEOREM 2.13 *If G acts on a set X and $x \in X$, then*

$$|\mathcal{O}_x| = |G : G_x|.$$

Proof
This follows by defining the map

$$\xi : G/G_x \to \mathcal{O}_x$$

with

$$\xi(gG_x) = g_\bullet x.$$

Note that ξ is well defined because given $g'G_x = gG_x$, we have $g' = gs$ for some $s \in G_x$. Observe that $s_\bullet x = x$ since $s \in G_x$. This gives

$$\xi(g'G_x) = g'_\bullet x = gs_\bullet x = g_\bullet(s_\bullet x) = g_\bullet x = \xi(gG_x),$$

showing that ξ is independent of the choice of the coset representatives and hence, ξ is well defined. Next, if $\xi(gG_x) = \xi(g'G_x)$, then $g_\bullet x = g'_\bullet x$. This yields $g^{-1}g'_\bullet x = x$ and so $g^{-1}g' \in G_x$ or $gG_x = g'G_x$. Hence ξ is injective. The function ξ is surjective because given $g_\bullet x \in \mathcal{O}_x$, we can choose gG_x to be its preimage under ξ. This implies that ξ is a bijection and

$$|\mathcal{O}_x| = |G : G_x|.$$

□

LEMMA 2.14 (i) Let G acts on a set X. If $x \in X$ and $\sigma \in G$ then $G_{\sigma x} = \sigma G_x \sigma^{-1}$.

(ii) If a finite group G acts on a finite set X and if x and y lie in the same orbit, then $|G_y| = |G_x|$.

Proof
Note that if $s \in G_x$ then

$$\sigma s\sigma^{-1}{}_\bullet(\sigma_\bullet x) = \sigma s_\bullet x = \sigma_\bullet x,$$

since $s_\bullet x = x$. This implies that $\sigma G_x \sigma^{-1} \subset G_{\sigma_\bullet x}$. Next, if $g \in G_{\sigma_\bullet x}$ then $g\sigma_\bullet x = \sigma_\bullet x$ This yields $\sigma^{-1} g \sigma_\bullet x = x$, or $G_{\sigma_\bullet x} \subset \sigma^{-1} G_x \sigma$. This completes the proof of (i).

Next, if x and y lie in the same orbit, we may write $y = \sigma_\bullet x$. By (i), we find that $\sigma G_x \sigma^{-1} = G_{\sigma_\bullet x} = G_y$. But there is a one to one correspondence between $\sigma G_x \sigma^{-1}$ and G_x since the map $\psi : G_x \to \sigma G_x \sigma^{-1}$ defined by $\psi(g) = \sigma g \sigma^{-1}$ has an inverse given by $\nu(g') = \sigma^{-1} g' \sigma$ for all $g' \in \sigma G_x \sigma^{-1}$.

□

THEOREM 2.15 Let G acts on a finite set X. If N is the number of orbits, then

$$N = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|,$$

where $\mathrm{Fix}(g)$ is the set of elements $x \in X$ fixed by g.

Proof
To prove the above, we consider

$$\begin{aligned} \sum_{\substack{g\in G, x\in X \\ g_\bullet x = x}} 1 &= \sum_{g\in G} \sum_{\substack{x\in X \\ g_\bullet x = x}} 1 \\ &= \sum_{g\in G} |\mathrm{Fix}(g)|. \end{aligned} \tag{2.4}$$

On the other hand,

$$\begin{aligned} \sum_{\substack{g\in G, x\in X \\ g_\bullet x = x}} 1 &= \sum_{x\in X} \sum_{\substack{g\in G \\ g_\bullet x = x}} 1 \\ &= \sum_{x\in X} |G_x| \\ &= \sum_{j=1}^{m} \sum_{x\in \mathcal{O}(j)} |G_x|, \end{aligned} \tag{2.5}$$

where $\mathcal{O}(j), 1 \le j \le m$ are the distinct orbits. Let $\mathcal{O}(j) = \mathcal{O}_{x_j}$ for some $x_j \in X$.

Since $|G_x| = |G_y|$ for any $x, y \in \mathcal{O}(j)$, we conclude that

$$\sum_{x \in \mathcal{O}(j)} |G_x| = \sum_{x \in \mathcal{O}(x_j)} |G_x| = |\mathcal{O}(x_j)||G_{x_j}| = |G : G_{x_j}||G_{x_j}| = |G|,$$

where the second last equality follows from Theorem 2.13. By (2.4) and (2.5), we deduce that

$$m = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|.$$

□

We are now ready to give another proof of Fermat's Little Theorem. Consider a p-gon where p is a prime. Suppose we want to color the vertices of the p-gon using n colors. How many ways can we do this?

Let X contains the p-tuples $(a_1, a_2, \cdots, a_p)$ where a_i takes one of the n colors. Let G be the cyclic group generated by $\sigma := (1, 2, \cdots, p)$. Let G acts on X by

$$\sigma^j \bullet (a_1, a_2, \cdots, a_p) = (a_{\sigma^j(1)}, a_{\sigma^j(2)}, \cdots, a_{\sigma^j(p)}).$$

Note that under this action, the orbit containing $(a_1, a_2, \cdots, a_p)$ are

$$\{(a_{i+1}, a_{i+2}, \cdots, a_p, a_1, \cdots, a_i), 0 \leq i \leq p-1\}.$$

This means that if a colored polygon can be obtained from another colored polygon via rotation, the two polygons would belong to the same orbit.

By Theorem 2.15, the number of such orbits is given by

$$\frac{1}{p}\left(|\mathrm{Fix}((1)(2)\cdots(p))| + |\mathrm{Fix}(\sigma)| + \cdots + |\mathrm{Fix}(\sigma^{p-1})|\right).$$

If $j \neq 0$, then σ^j is a p-cycle since p is a prime. A n-colored polygon with p-vertices is fixed by a p-cycle only if the vertices are colored with the same color. This implies that the number of $x \in X$ fixed by σ^j is exactly n for each $j \neq 0$ as there are only n polygons with all vertices having the same color.

The number of x fixed by $(1)(2)\cdots(p)$ is n^p since all $x \in X$ are fixed by the identity of G. Since the number of orbits is an integer, we find that

$$n^p \equiv n \pmod{p},$$

and this yields Fermat's Little Theorem.

3 Multiplicative Functions

3.1 Multiplicative functions and even perfect numbers

DEFINITION 3.1 An *arithmetical function* f is a function from $\mathbf{N}$ to $\mathbf{C}$.

DEFINITION 3.2 An arithmetical function f is said to be *completely multiplicative* if $f(1) = 1$ and for all positive integers m and n,

$$f(mn) = f(m)f(n).$$

EXAMPLE 3.1 The functions $N(n) = n$ and $u(n) = 1$ are completely multiplicative and therefore multiplicative. The function $\varphi(n)$ is multiplicative but not completely multiplicative.

DEFINITION 3.3 An arithmetical function f is said to be *multiplicative* if $f(1) = 1$ and when $(m, n) = 1$,

$$f(mn) = f(m)f(n).$$

All completely multiplicative functions are multiplicative functions. We have already seen that $\varphi(n)$ is multiplicative but we will not assume this fact in this chapter. In fact, the purpose of this chapter is to study some properties of multiplicative function and show that $\varphi(n)$ without using the Chinese Remainder Theorem. There are of course simpler multiplicative functions. We will encounter one of them in the next section.

3.2 Multiplicative function and perfect numbers

LEMMA 3.1 Let $(m,n)=1$ and a be any positive integer. Then $(a,m)(a,n)=(a,mn)$.

Proof
It suffices to show that

$$\left(\frac{a}{(a,m)(a,n)},\frac{m}{(a,m)}\frac{n}{(a,n)}\right)=1.$$

First observe that $(a,m)|a$ and $(a,n)|a$ and since $(m,n)=1$, we have $((a,m),(a,n))=1$ and this implies that $(a,m)(a,n)|a$. In other words, $\dfrac{a}{(a,m)(a,n)}$ is an integer. Next, $\dfrac{a}{(a,m)}$ and $\dfrac{m}{(a,m)}$ are relatively prime implies that

$$\left(\frac{a}{(a,m)(a,n)},\frac{m}{(a,m)}\right)=1.$$

Similarly,

$$\left(\frac{a}{(a,m)(a,n)},\frac{n}{(a,n)}\right)=1.$$

Combining the last two identities yields

$$\left(\frac{a}{(a,m)(a,n)},\frac{m}{(a,m)}\frac{n}{(a,n)}\right)=1.$$

□

When $(m,n)=1$ and $d|mn$, the above lemma shows that d can be written uniquely in the form d_1d_2 with $d_1|m$ and $d_2|n$. To see this, we observe that

$$d=(d,mn)=(d,m)(d,n),$$

which implies that $d=d_1d_2$ with $d_1|m$ and $d_2|n$. Next, we prove uniqueness of such representation. Suppose $d=d_1'd_2'$, $d_1'|m$ and $d_2'|n$. Then

$$(d,m)=(d_1'd_2',m)=(d_1',m)=d_1'$$

since $(m,n)=(m,d_2')=1$. Similarly,

$$(d,n)=d_2'$$

and this shows that the representation of $d=d_1d_2$ with $d_1|m$ and $d_2|n$ is unique.

The symbol $\displaystyle\sum_{d|n}f(d)$ denotes the sum of $f(d)$ over all divisors of n.

THEOREM 3.2 If f is multiplicative, then $\displaystyle\sum_{d|n}f(d)$ is multiplicative.

Proof
Let $g(n) = \sum_{d|n} f(d)$. Then

$$g(mn) = \sum_{d|mn} f(d) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1 d_2)$$

$$= \sum_{\substack{d_1|m \\ d_2|n}} f(d_1)f(d_2) = \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) = \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) = g(m)g(n).$$

□

DEFINITION 3.4 Let α be an integer. Let $\sigma_\alpha(1) = 1$ and

$$\sigma_\alpha(n) = \sum_{d|n} d^\alpha.$$

Note that $\sigma_0(n) = d(n)$. When $\alpha = 1$, we write

$$\sigma(n) := \sum_{d|n} d = \sigma_1(n).$$

This is the sum of all divisors of n.

EXAMPLE 3.2 Show that $\sigma_\alpha(n)$ is multiplicative.

Solution
The function n^α is multiplicative. Since $\sigma_\alpha(n) = \sum_{d|n} d^\alpha$ then $\sigma_\alpha(n)$ is multiplicative by Theorem 3.2.

EXAMPLE 3.3 Let $n = \prod_{p|n} p^{\beta_p}$. Show that

$$d(n) = \prod_{p|n} (1 + \beta_p) \text{ and } \sigma(n) = \prod_{p|n} \frac{p^{\beta_p+1} - 1}{p - 1}.$$

Solution
Since $d(n)$ is multiplicative, it suffices to show that $d(p^{\beta_p}) = (1 + \beta_p)$. Now,

the divisors of p^{β_p} are $1, p, p^2, \cdots, p^{\beta_p}$ and so, p^{β_p} has exactly $1+\beta_p$ divisors. Furthermore,

$$\sigma(p^{\beta_p}) = 1 + p + \cdots p^{\beta_p} = \frac{p^{\beta_p+1}-1}{p-1}$$

and this completes the proof of the second formula.

3.3 Perfect numbers

DEFINITION 3.5 A positive integer n is called a *perfect number* if it is the sum of all its divisors $d \neq n$.

THEOREM 3.3 A positive even integer N is perfect if and only if $N = 2^{k-1}(2^k - 1)$ where $2^k - 1$ is prime.

Proof

First, we observe N is a perfect number if and only if

$$\sigma(N) = 2N.$$

Now, if $N = 2^{k-1}(2^k-1)$ with 2^k-1 a prime, then the divisors of N are $2^j, 0 \leq j \leq k-1$ and $2^j(2^k-1), 0 \leq j \leq k-1$. The sum of divisors is

$$2^k - 1 + (2^k-1)(2^k-1) = 2^k(2^k-1) = 2N.$$

Hence, N is perfect.

Conversely, if N is even and perfect. Write $N = 2^{k-1}m$, $k \geq 2$ and m odd. Since $\sigma(n)$ is multiplicative and $(2^{k-1}, m) = 1$, we conclude that

$$\sigma(N) = \sigma(2^{k-1})\sigma(m) = \left(1 + 2 + \cdots + 2^{k-1}\right)\sigma(m) = (2^k-1)\sigma(m). \tag{3.1}$$

But N is perfect and this implies that

$$\sigma(N) = 2N = 2^k m. \tag{3.2}$$

From (3.1) and (3.2), we deduce that

$$(2^k-1)\sigma(m) = 2^k m.$$

Since $(2^k-1, 2^k) = 1$, by Euclid's Lemma, we deduce that

$$(2^k-1) | m. \tag{3.3}$$

By (3.3), we may write

$$m = (2^k-1)s, \tag{3.4}$$

with $s \geq 1$. With this expression for m, we find using (3.1) and (3.2) that

$$\sigma(m) = 2^k s. \tag{3.5}$$

If $s > 1$ then (3.4) shows that 1, s and $(2^k - 1)s$ are divisors of m. Hence,

$$\sigma(m) \geq 1 + s + (2^k - 1)s > s + (2^k - 1)s = 2^k s.$$

This contradicts (3.5). Therefore $s = 1$, $m = 2^k - 1$ and $\sigma(m) = 2^k$. But this means that 1 and $2^k - 1$ are the only divisors of m and hence $m = 2^k - 1$ must be a prime. □

3.4 The function $\mu(n)$ and further properties of multiplicative functions

DEFINITION 3.6 Let f and g be two arithmetical functions. We define the *Dirichlet product* of f and g, denoted by $f * g$, as

$$(f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d}).$$

REMARK 3.4 Suppose $d_1, d_2, \cdots, d_k$ are the divisors of n, then

$$\sum_{d|n} f(d)g(n/d) = f(d_1)f(n/d_1) + f(d_2)g(n/d_2) + \cdots + f(d_k)g(n/d_k).$$

Now, each d_j can be written in the form n/d'_j, where d'_j is the conjugate divisor of d_j.Hence,

$$\sum_{d|n} f(d)g(n/d) = \sum_{d'|n} f(n/d')g(d').$$

Therefore

$$\sum_{d|n} f(d)g(n/d) = \sum_{d|n} f(n/d)g(d). \tag{3.6}$$

THEOREM 3.5 Let f and g be multiplicative. Then $f * g$ is multiplicative.

Proof
The proof is similar to the proof that $\sigma_\alpha(n)$ is multiplicative. More precisely, if

$H(n) = f * g(n)$, then

$$H(mn) = \sum_{d|mn} f(d)g(n/d) = \sum_{d_1 d_2|mn} f(d_1 d_2) g\left(\frac{m}{d_1} \cdot \frac{n}{d_2}\right)$$
$$= \sum_{d_1|m} f(d_1) g\left(\frac{m}{d_1}\right) \sum_{d_2|n} f(d_2) g\left(\frac{n}{d_2}\right) = H(m)H(n).$$

□

We now give an application of the observation that $f * g$ is multiplicative if f and g are multiplicative.

DEFINITION 3.7 The *Möbius function* $\mu(n)$ defined by $\mu(1) = 1$ and for $n = \prod_{k=1}^{m} p_k^{\alpha_k}$,

$$\mu(n) = \begin{cases} (-1)^m & \text{if } \alpha_i = 1, 1 \le i \le m \\ 0 & \text{otherwise.} \end{cases}.$$

Note that $\mu(n)$ is a multiplicative function.

THEOREM 3.6 Let $\mu(n)$ be the Möbius function. Then

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{otherwise.} \end{cases} \tag{3.7}$$

Proof
First, we note that the left hand side (3.7) is $\mu * u$ where $u(n) = 1$ for all positive integers n. From Theorem 3.5, we know that $\mu * u$ is multiplicative. Hence $\mu * u(1) = 1$. To determine $\mu * u(n)$ for $n > 1$, it suffices to determine the values of $\mu * u$ at prime powers. Now,

$$\sum_{d|p^\alpha} \mu(d) = 1 - 1 = 0,$$

if $\alpha \ge 1$. Hence $\mu * u(n) = 0$ for $n > 1$. □

Note that the right hand side of (3.7) can be written as $[1/n]$ where, $[x]$ is the integer part of x.

DEFINITION 3.8 For positive integer n, we define $I(n) = [1/n]$.

Theorem 3.6 can be written as

$$\mu * u = I. \tag{3.8}$$

Next, we will show that $\varphi(n)$ is multiplicative using Theorem 3.5.

THEOREM 3.7 For positive integers m and n such that $(m, n) = 1$,

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Proof
Note that

$$\begin{aligned}\varphi(n) &= \sum_{\substack{k=1\\(k,n)=1}}^{n} 1 = \sum_{k=1}^{n}\left[\frac{1}{(k,n)}\right]\\ &= \sum_{k=1}^{n}\sum_{\ell|(k,n)}\mu(\ell) = \sum_{\ell|n}\mu(\ell)\sum_{\substack{k=1\\ \ell|k}}^{n} 1\\ &= \sum_{\ell|n}\mu(\ell)\frac{n}{\ell}.\end{aligned}$$

Hence $\varphi(n)$ is the Dirichlet product of the multiplicative functions $\mu(n)$ and $N(n)$ and by Theorem 3.5, $\varphi(n)$ is multiplicative. □

REMARK 3.8 Note that in the above proof that $\varphi(n)$ is multiplicative, we avoid the use of the Chinese Remainder Theorem. Furthermore, when $n = p^\alpha$, the above formula gives

$$\varphi(p^\alpha) = \sum_{d|p^\alpha}\mu(d)p^\alpha/d = p^\alpha - p^{\alpha-1}.$$

EXAMPLE 3.4 Let n be an even positive integer. Show that $\sum_{d|n}\mu(d)\varphi(d) = 0$.

Solution

Since n is even $2^a|n$ for some positive integer a. Now, if $F(n) = \sum_{d|n}\mu(d)\varphi(d)$, then $F(n)$ is multiplicative and $F(n) = F(2^a)F(m)$ if we write $n = 2^a m$ with $(m, 2) = 1$. But $F(2^a) = \mu(1)\varphi(1) + \mu(2)\varphi(2) = 0$. Therefore $F(n) = 0$.

3.5 The identity for the Dirichlet product, associativity and the Möbius inversion formula

THEOREM 3.9 Let $I(n)$ be given by $[1/n]$. The function I is the identity function for $*$, that is, $I * f = f * I = f$ for every arithmetical function f.

Proof
By the definition of I, we find that

$$(I * f)(n) = \sum_{d|n} I(d) f\left(\frac{n}{d}\right) = f(n).$$

By the commutative law in Theorem 3.10, we conclude that

$$f * I = f.$$

□

THEOREM 3.10 The Dirichlet product is commutative and associative, that is, for any arithmetical functions f, g, k, we have

$$f * g = g * f$$

and

$$(f * g) * k = f * (g * k).$$

Proof
The Dirichlet product of f and g is given by

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

Let $d_1 = n/d$ be the conjugate divisor of d. As d runs through all divisors of n, so does d_1. By (3.6),

$$(f * g)(n) = \sum_{d_1|n} f\left(\frac{n}{d_1}\right) g(d_1) = (g * f)(n).$$

To prove the associativity property, let $A = g * k$ and consider $f * A = f * (g * k)$.

We have

$$\begin{aligned}(f * A)(n) &= \sum_{a|n} f(a) A\left(\frac{n}{a}\right) \\ &= \sum_{a\cdot d=n} f(a) \sum_{b\cdot c=d} g(b)k(c) \\ &= \sum_{a\cdot b\cdot c=n} f(a)g(b)k(c).\end{aligned}$$

Similarly, if we set $B = (f * g)$ and consider $B * k$, we have

$$\begin{aligned}(B * k)(n) &= \sum_{d\cdot c=n} B(d)k(c) \\ &= \sum_{d\cdot c=n} \sum_{a\cdot b=d} f(a)g(b)k(c) \\ &= \sum_{a\cdot b\cdot c=n} f(a)g(b)k(c).\end{aligned}$$

Therefore,

$$(f * (g * k))(n) = ((f * g) * k)(n).$$

□

THEOREM 3.11 (The Möbius inversion formula) If $f = g * u$, then $g = f * \mu$. Conversely, $g = f * \mu$ implies that $f = g * u$.

Proof

Suppose $f = g * u$. Then by (3.8), Theorem 3.10 and Theorem 3.9, we deduce that

$$f * \mu = (g * u) * \mu = g * (u * \mu) = g * I = g.$$

Conversely, if $g = f * \mu$ then

$$g * u = (f * \mu) * u = f * (\mu * u) = f * I = f.$$

□

EXAMPLE 3.5 Show that

$$n = \sum_{d|n} \varphi(d).$$

Solution

This follows from the above theorem and the fact that

$$\varphi(n) = \mu * N(n)$$

where $N(k) = k$.

EXAMPLE 3.6 Show that $\sigma = \varphi * d$.

Solution

Note that $\varphi * d = (N * \mu) * (u * u)$. By associativity of $*$, $(N * \mu) * (u * u) = ((N * \mu) * u) * u = (N * (\mu * u)) * u = (N * I) * u = N * u = \sigma$.

4 The Bertrand Postulate

4.1 The function [x]

DEFINITION 4.1 The function $[x]$ is defined as the integer part of a real number x.

REMARK 4.1 When $x > 0$, this function coincides with the more familiar floor function $\lfloor x \rfloor$ which gives the integer less than x. Note that $[x]$ is NOT an arithmetical function since its domain is not a subset of the set of integers. The function $I(n)$, however, is an arithmetical function in terms of $[x]$.

We now give two results where $[x]$ appears.

LEMMA 4.2 Let α be the exponent of p in the factorization of $n!$. Then

$$\alpha = \sum_{j=1}^{k} \left[\frac{n}{p^j} \right],$$

where k is given by the inequality $p^k \leq n < p^{k+1}$.

Proof
The number of integers less than or equal to n and divisible by m is $\left[\frac{n}{m}\right]$. Therefore, the number of integers from 1 to n that is exactly a multiple of p^j is

$$\left[\frac{n}{p^j} \right] - \left[\frac{n}{p^{j+1}} \right].$$

Hence, the exponent of p in $n!$ is

$$\left(\left[\frac{n}{p} \right] - \left[\frac{n}{p^2} \right] \right) + 2 \left(\left[\frac{n}{p^2} \right] - \left[\frac{n}{p^3} \right] \right) + \cdots + (k-1) \left(\left[\frac{n}{p^{k-1}} \right] - \left[\frac{n}{p^k} \right] \right) + k \left[\frac{n}{p^k} \right]$$
$$= \left[\frac{n}{p} \right] + \left[\frac{n}{p^2} \right] + \cdots + \left[\frac{n}{p^k} \right],$$

where k is such that

$$p^k \leq n < p^{k+1}.$$

□

DEFINITION 4.2 Let $x \geq 0$. The function $\{x\}$ is defined as the fractional part of x and it is given by $\{x\} = x - [x]$. The number $\{x\}$ satisfies $0 \leq \{x\} < 1$.

LEMMA 4.3 Let n and $k \leq n$ be positive integers. Then

$$\left[\frac{2n}{k}\right] - 2\left[\frac{n}{k}\right] = 0 \quad \text{or} \quad 1.$$

Proof
Note that $2n/k = [2n/k] + \{2n/k\}$ and $n/k = [n/k] + \{n/k\}$. Therefore,

$$0 = 2n/k - 2(n/k) = [2n/k] - 2[n/k] + \{2n/k\} - 2\{n/k\}.$$

Since $0 \leq \{x\} < 1$, we conclude that $-2 < \{2n/k\} - 2\{n/k\} < 1$, and therefore, $\{2n/k\} - 2\{n/k\} = -1$ or 0 and this implies that $[2n/k] - 2[n/k] = 0$ or 1. □

REMARK 4.4 The above lemmas will be used later in this chapter.

4.2 Bertrand's postulate and three Lemmas

We begin with a simple example.

EXAMPLE 4.1 Let $n > 2$ be a positive integer. Then there exists a prime in the interval $(n, n!)$.

Solution

Suppose there are no prime in the interval $(n, n!)$. This implies that if $q|(n! - 1)$ then $q \leq n$. But if $q \leq n$ then $q|n!$ this implies that $n! - 1 \equiv 0 \pmod{q}$ and $n! \equiv 0 \pmod{q}$ which implies that $q = 1$, a contradiction. Therefore, there must be a prime in the interval $(n, n!)$.

REMARK 4.5 This implies that there are infinitely many primes and the proof is similar to Euclid's proof.

The question we can ask now is whether we can shorten the interval $(n, n!)$ and make the same conclusion. It turns out that we can. The fact which is known as Bertrand's Postulate:

THEOREM 4.6 Let $n \geq 2$ be any positive integer. There is at least a prime in the interval $(n, 2n)$.

We will give Erdös' proof of Theorem 4.6 after proving a few important lemmas.

LEMMA 4.7 Let $r(p)$ satisfies

$$p^{r(p)} \leq 2n < p^{r(p)+1}. \tag{4.1}$$

Then

$$\binom{2n}{n} \Big| \prod_{p \leq 2n} p^{r(p)}.$$

Proof

By Lemma 4.2, the exponent of p in $n!$ is $\sum_{j=1}^{k} [n/p^j]$, where k is such that

$$p^k \leq n < p^{k+1}.$$

Therefore the exponent of p in $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ is

$$\sum_{j=1}^{r(p)} \left\{ \left[\frac{2n}{p^j} \right] - 2 \left[\frac{n}{p^j} \right] \right\}.$$

By Lemma 4.3, $[2n/p^j] - 2[n/p^j] = 0$ or 1 and hence,

$$\sum_{j=1}^{r(p)} \left\{ \left[\frac{2n}{p^j} \right] - 2 \left[\frac{n}{p^j} \right] \right\} \leq \sum_{j=1}^{r(p)} 1 = r(p).$$

Therefore,

$$\binom{2n}{n} \Big| \prod_{p \leq 2n} p^{r(p)}.$$

□

LEMMA 4.8 If $p > 2$ and

$$\frac{2n}{3} < p \leq n,$$

then

$$p \nmid \binom{2n}{n}.$$

Proof
If p satisfies

$$\frac{2n}{3} < p \leq n,$$

then p occurs once in the factorization of $n!$. This is because if $2p \leq n$, then

$$p \leq \frac{n}{2} < \frac{2n}{3} < p,$$

which is a contradiction to our assumption. Now p occurs twice in $(2n)!$ because $3p > 2n$. Therefore,

$$p \nmid \binom{2n}{n}.$$

□

LEMMA 4.9 For $n \geq 2$,

$$\prod_{p \leq n} p < 4^n.$$

Proof

Let $P(n)$ denote the statement "$\prod_{p \leq k} 4^k$". It is clear that $P(2)$ and $P(3)$ are true. If $m > 1$, then

$$\prod_{p \leq 2m+2} p = \prod_{p \leq 2m+1} p \leq 4^{2m+1} < 4^{2m+2}.$$

Therefore,

$$P(2m+1) \text{ implies } P(2m+2).$$

Suppose $n = 2m+1$. Then each prime in the interval $[m+2, 2m+1]$ is a factor of $\binom{2m+1}{m}$. This is because primes in the interval do not occur in the denominator of $\binom{2m+1}{m}$ (which is $m!(m+1)!$).

Since $P(m+1)$ holds, we find that

$$\prod_{p \leq 2m+1} p = \prod_{m+2 \leq p \leq 2m+1} p \prod_{p \leq m+1} p \leq \binom{2m+1}{m} 4^{m+1}.$$

But,

$$(1+1)^{2m+1} = \binom{2m+1}{0} + \binom{2m+1}{1} + \cdots + \binom{2m+1}{m} + \binom{2m+1}{m+1} + \cdots + \binom{2m+1}{2m+1} \geq 2\binom{2m+1}{m}.$$

Therefore,

$$\binom{2m+1}{m} < 4^m.$$

Hence,

$$\prod_{p \leq 2m+1} p \leq 4^m \cdot 4^{m+1} = 4^{2m+1}$$

and $P(2m+1)$ is true. □

4.3 Erdös' Proof of Theorem 4.6

In this section, we prove Bertrand's postulate.

Suppose that Bertrand's postulate is false. Then there exists a positive integer $n > 1$ such that there is no prime p in the interval $[n, 2n)$. By Lemma 4.8, all prime factors of

$$\binom{2n}{n}$$

must satisfy $p \leq 2n/3$. Let $s(p)$ be the largest prime power of p that divides $\binom{2n}{n}$. By Lemma 4.7,

$$\prod_{p \leq 2n/3} p^{s(p)} = \binom{2n}{n} \mid \prod_{p \leq 2n} p^{r(p)}.$$

Therefore, $s(p) \leq r(p)$ and

$$p^{s(p)} \leq p^{r(p)} \leq 2n \tag{4.2}$$

by (4.1). If $s(p) > 1$, then $p^{s(p)} \geq p^2$ and thus,

$$p < \sqrt{2n}$$

since $p^{s(p)} < 2n$. In other words, no more than $[\sqrt{2n}]$ primes occur in $\binom{2n}{n}$ with

exponent larger than 1. Now,

$$\begin{aligned}\binom{2n}{n} &= \prod_{p\le 2n/3} p^{s(p)} = \prod_{\substack{p\le 2n/3\\ s(p)>1}} p^{s(p)} \prod_{\substack{p\le 2n/3\\ s(p)=1}} p^{s(p)}\\ &\le \prod_{p<\sqrt{2n}} p^{s(p)} \prod_{p\le 2n/3} p\\ &< (2n)^{[\sqrt{2n}]} 4^{[2n/3]},\end{aligned}$$

by (4.2) and Lemma 4.9.

Next, since

$$(1+1)^{2n} = \binom{2n}{0} + \cdots + \binom{2n}{n} + \cdots + \binom{2n}{2n} < (2n+1)\binom{2n}{n},$$

we conclude that

$$\frac{4^n}{2n+1} \le \binom{2n}{n} \le (2n)^{\sqrt{2n}} 4^{2n/3},$$

which implies that

$$4^{n/3} \le (2n+1)^{\sqrt{2n}+1}.$$

Therefore,

$$n\frac{\ln 4}{3} < (\sqrt{2n}+1)\ln(2n+1).$$

The above inequality is true for only small values of n, for example, $n < 469$. This implies that for $n \ge 750$, Bertrand's postulate is true. For $n < 750$, we verify directly that Bertrand's postulate is true by observing that 3 is a prime between 2 and 4, 5 is a prime between 3 and 6, 7 is a prime between 5 and 10, 13 is a prime between 7 and 14, 23 is a prime between 13 and 26, 43 is a prime between 23 and 46, 83 is a prime between 43 and 85, 163 is a prime between 83 and 166, 317 is a prime between 163 and 326, 631 is a prime between 317 and 634.

EXAMPLE 4.2 Prove that $n! = m^k$ is impossible in integers for $k > 1, m > 1, n > 1$.

Solution

The claim is true for $n \ge 5$. Suppose $n = 2j$ or $2j+1$. By Bertrand's postulate, there exists a prime p between j and $2j$. The exponent of p in $n!$ is 1. If $n! = m^k$, then $p|m^k$ which by Euclid's Lemma would imply that $p|m$. This means that the exponent of p in m^k is greater than 1, which contradicts that p divides $n!$ but $p^2 \nmid n!$. Therefore, $n! = m^k$ with $k > 1$ is not solvable in $n > 1$ and $m > 1$.

EXAMPLE 4.3 Let $n \geq 4$. Then the product of the first $n-1$ primes is greater than the square of the n-th prime. In other words, $\prod_{j=1}^{n-1} p_j \geq p_n^2$.

Solution

The claim is true for $n = 4$ since $2 \cdot 3 \cdot 5 \cdot 7 = 210 > 121 = 11^2$. Suppose the claim is true for $k = n - 1$. Then $p_{n+1} < 2p_n$ or

$$p_{n+1}^2 < 4p_n^2 < 4p_1 \cdot p_2 \cdot \cdots \cdot p_{n-1} < p_1 \cdot p_2 \cdot \cdots \cdot p_{n-1} \cdot p_n,$$

where we have used the fact that $p_n \geq 7 > 4$.

5 Congruence equations

5.1 Congruence equations

Let $f(x)$ be a polynomial with coefficients in $\mathbf{Z}$. A congruence equation is of the form

$$f(x) \equiv 0 \pmod{m},$$

where m is a positive integer. In this Chapter, we will study such equations.

THEOREM 5.1 Let $f(x)$ be a fixed polynomial with integral coefficients, and for any positive integer m let $N_f(m)$ denote the number of solutions of the congruence

$$f(x) \equiv 0 \pmod{m}.$$

If $m = m_1 m_2$ where $(m_1, m_2) = 1$, then $N_f(m) = N_f(m_1)N_f(m_2)$. If $m = \prod_p p^{\alpha_p}$ is the canonical factorization of m, then

$$N_f(m) = \prod_p N_f(p^{\alpha_p}).$$

Proof
Let m be a positive integer. Suppose $(m_1, m_2) = 1$ and that there are $N_f(m_1)$ solutions, say $\{a_1, \cdots, a_{N_f(m_1)}\}$, to

$$f(x) \equiv 0 \pmod{m_1}$$

and $N_f(m_2)$ solutions, say $\{b_1, \cdots, b_{N_f(m_2)}\}$, to the equation

$$f(x) \equiv 0 \pmod{m_2}.$$

To each pair of solutions (a_i, b_j) there exists an integer c_{ij} modulo m such that

$$f(c_{ij}) \equiv 0 \pmod{m_1}$$

and

$$f(c_{ij}) \equiv 0 \pmod{m_2}.$$

The existence of c_{ij} is guaranteed by the Chinese Remainder Theorem. This implies that

$$f(c_{ij}) \equiv 0 \pmod{m}$$

and therefore

$$N_f(m_1)N_f(m_2) \leq N_m(f).$$

Next, if

$$f(x) \equiv 0 \pmod{m}$$

and $m = m_1m_2, (m_1, m_2) = 1$, then by Chinese Remainder Theorem, there are $N_f(m)$ pairs $(a \mod m_1, b \pmod{m_2})$ such that

$$f(a) \equiv 0 \pmod{m_1}$$

and

$$f(b) \equiv 0 \pmod{m_2}.$$

This implies that

$$N_f(m) \leq N_f(m_1)N_f(m_2).$$

Hence,

$$N_f(m_1m_2) = N_f(m_1)N_f(m_2).$$

□

EXAMPLE 5.1 Let $f(x) = x^2 + x + 3$. Find all roots of the congruence $f(x) \equiv 0 \pmod{15}$.

Solution

The solutions for $f(x) \equiv 0 \pmod{15}$ are $3, 6, 8, 11$. The solutions for $f(x) \equiv 0 \pmod{3}$ are 0 and 2 and for $f(x) \equiv 0 \pmod{5}$ are 1 and 3. Note that $N_f(15) = N_f(3)N_f(5)$.

5.2 Prime power moduli

Theorem 5.1 shows that in order to solve

$$f(x) \equiv 0 \pmod{m},$$

it suffices to solve

$$f(x) \equiv 0 \pmod{p^\alpha} \tag{5.1}$$

for $p^\alpha \| m$ where p is a prime.

We now show that in order to solve (5.1), if suffices to find the solutions of

$$f(x) \equiv 0 \pmod{p}.$$

By Taylor's series expansion,

$$f(a+tp^j) = f(a) + tp^j f'(a) + t^2 p^{2j} f''(a)/2 + \cdots + t^n p^{nj} f^{(n)}(a)/n!, \tag{5.2}$$

where n is the degree of $f(x)$. Observe that if

$$f(x) = \sum_{r=0}^{n} c_r x^r,$$

then

$$\frac{f^{(k)}(x)}{k!} = \sum_{r=k}^{n} c_r \binom{r}{k} x^{r-k}.$$

Therefore,

$$\frac{f^{(k)}(a)}{k!}$$

is an integer for $0 \le k \le n$.

Let a be an integer that satisfies the congruence

$$f(a) \equiv 0 \pmod{p^j}.$$

In other words,

$$p^j | f(a). \tag{5.3}$$

Next, suppose $f(a+tp^j) \equiv 0 \pmod{p^{j+1}}$. Since

$$t^k p^{kj} \frac{f^{(k)}(a)}{k!} \equiv 0 \pmod{p^{j+1}},$$

for $k > 1$ ($2j > j$ for $j \ge 1$), we conclude from (5.2) that

$$0 \equiv f(a+tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}},$$

which implies that

$$tf'(a) \equiv -\frac{f(a)}{p^j} \pmod{p}. \tag{5.4}$$

Note that the right hand side of (5.4) is an integer by (5.3). We now split our investigation into cases:

Case 1.

If $p | f'(a)$ but $p \nmid \dfrac{f(a)}{p^j}$ then (5.4) is not solvable.

Case 2.

If $p | f'(a)$ and $p | \dfrac{f(a)}{p^j}$ then there are p solutions for t in (5.4).

Case 3. $p \nmid f'(a)$.

In this case, there is a unique solution t for (5.4) and hence we obtain

THEOREM 5.2 (Hensel's Lemma) Suppose that $f(x)$ is a polynomial with integral coefficient. If $f(a) \equiv 0 \pmod{p^j}$ and $f'(a) \not\equiv 0 \pmod{p}$, then there is a unique $t \pmod{p}$ such that $f(a + tp^j) \equiv 0 \pmod{p^{j+1}}$.

REMARK 5.3 Note that if u is solution of

$$f(x) \equiv 0 \pmod{p^{j+1}}, \tag{5.5}$$

then by division algorithm, we can write $u = a + tp^j$ for some a and t where $0 \leq a < p^j$ and $0 \leq t \leq p$, we conclude that all solutions of (5.5) are of the form $a + tp^j$, with

$$f(a) \equiv 0 \pmod{p^j}, \tag{5.6}$$

and so, we have exhausted all possible solutions to (5.5) by considering solutions of (5.6).

EXAMPLE 5.2 Solve $x^3 - 2x^2 + 3x + 9 \equiv 0 \pmod{3^3}$.

Solution

The solutions to the congruence

$$f(x) \equiv 0 \pmod{3}$$

are $x = 0$ and 2.

Now,

$$f'(x) = 3x^2 - 4x + 3.$$

Since $f'(2) \not\equiv 0 \pmod{3}$, we see that there is a unique solution arising for $x = 2$. We need to solve

$$7t \equiv -15/3 \pmod{3}$$

and it turns out that $t = 1$. The solution for the congruence $f(x) \equiv 0 \pmod{p}$ arising from $x = 2$ is therefore $2 + 3 = 5$.

Now

$$f'(0) = 3 \quad \text{and} \quad f(0) = 9.$$

Hence there are three solutions for

$$f(x) \equiv 0 \pmod{9}$$

corresponding to the solution $x = 0$ from

$$f(x) \equiv 0 \pmod{3}.$$

These are $x = 0, 3$ and 6.

We now have four solutions for

$$f(x) \equiv 0 \pmod{3^2}.$$

We check that $f(0) = 9$ and $f'(0) = 3$ and so

$$f(x) \equiv 0 \pmod{27}$$

has no solution arising from $x = 0$.

Next, $f(3) = 27$ and $f'(3) = 18$ and so, there are three solutions arising from $x = 3$. These are $x = 3, 12$ and 21.

For $x = 6$ we have $f(6) = 171$ and $f'(6) = 87$. But $3 \nmid (171/9)$ and hence, there are no solutions arising from $x = 6$.

For $x = 5$ we find that $f(5) = 99$ and $f'(5) = 58$ and we need to solve the congruence

$$58t \equiv -11 \pmod{3}.$$

The solution is $t = 1$ and so 14 is the solution for the congruence.

In conclusion the solutions to the congruence

$$f(x) \equiv 0 \pmod{27}$$

are 3,12,14 and 21.

5.3 Prime moduli

In the previous section, we have seen that we can reduce the problem of finding solutions for $f(x) \equiv 0 \pmod{p^\alpha}$ to finding solutions for $f(x) \equiv 0 \pmod{p}$.

We will first prove a result for polynomials over a field $\mathbf{F}$, that is an analogue for the Division Algorithm for integers.

THEOREM 5.4 Given the polynomials $f(x), g(x) \in \mathbf{F}[x]$, where deg $g(x) > 0$, there exist polynomials $q(x), r(x) \in \mathbf{F}[x]$ such that

$$f(x) = g(x)q(x) + r(x),$$

with either $r(x) = 0$ or $0 \leq \deg r(x) < \deg g(x)$.

Proof

We proceed by induction on deg $f(x)$. First fix the polynomial $g(x)$. Suppose $f(x) = 0$ or deg $f(x) <$ deg $g(x)$, then $f(x) = 0 \cdot g(x) + f(x)$. So we may assume that deg $f(x) \geq$ deg $g(x)$.

Suppose the statement is true for any polynomials with degrees less than or equal to $n-1$. Let $f(x)$ be a polynomial of degree n. Write

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

and

$$g(x) = b_0 + b_1 x + \cdots + b_m x^m,$$

with $a_n \neq 0$ and $b_m \neq 0$ and $n \geq m$. Since $\mathbf{F}$ is a field, b_m^{-1} exists and the polynomial

$$P(x) := f(x) - b_m^{-1} a_n x^{n-m} g(x) \qquad (*)$$

has degree $n-1$. Hence, there exist $q(x)$ and $r(x)$ such that

$$P(x) = q(x)g(x) + r(x),$$

with $\deg r(x) = 0$ or $\deg r(x) < \deg g(x)$. But by (*),

$$f(x) = (q(x) + b_m^{-1} a_n x^{n-m})g(x) + r(x),$$

hence the result.

□

We now let $\mathbf{F}$ be the finite field $\mathbf{F}_p := \mathbf{Z}/p\mathbf{Z}$. Let $g(x)$ be the polynomial $x^p - x$ and suppose the degree of $f(x)$ is $n \geq p$. By Theorem 5.4, we conclude that

$$f(x) = (x^p - x)q(x) + r(x),$$

with $q(x), r(x) \in \mathbf{F}_p[x]$ and $0 \leq \deg r(x) < p$.

Suppose u is such that

$$f(u) \equiv 0 \pmod{p}.$$

By Fermat's Little Theorem, we find that $u^p - u \equiv 0 \pmod{p}$. Therefore, $r(u) \equiv 0 \pmod{p}$. Conversely, if $r(u) \equiv 0 \pmod{p}$, then $f(u) \equiv 0 \pmod{p}$. This shows that to study $f(x) \equiv 0 \pmod{p}$, it suffices to consider those polynomial $f(x)$ with $\deg f(x) < p$.

THEOREM 5.5 (Lagrange) Let p be a prime and $f(x)$ be a non-zero polynomial. If the degree of $f(x)$ is $n < p$, then the congruence

$$f(x) \equiv 0 \pmod{p} \tag{5.7}$$

has at most n solutions.

Proof

We prove this by induction on the degree of $f(x)$. If $n = 0$, $a_0 \not\equiv 0 \pmod{p}$ implies that there are no solution to (5.7). If the degree of $f(x)$ is 1, then we see that we are solving

$$a_1 x + a_2 \equiv 0 \pmod{p}.$$

This is solvable since $a_1 \not\equiv 0 \pmod{p}$. Therefore the number of solution is 1. Suppose the result holds for all polynomials of degree less than n. Let $f(x)$ be a polynomial of degree n. If $f(x) \equiv 0 \pmod{p}$ has no solution, then we are done. Next, suppose u be a root of the n-th degree polynomial f. Then by the division algorithm for $\mathbf{F}_p[x]$,

$$f(x) = (x-u)g(x) + r_0$$

for some polynomial $g(x)$ of degree $n-1$. Hence,

$$r_0 \equiv 0 \pmod{p}$$

since

$$f(u) \equiv 0 \pmod{p} \quad \text{and} \quad (u-u)g(u) \equiv 0 \pmod{p}.$$

Therefore,

$$f(x) \equiv (x-u)g(x) \pmod{p}.$$

Next, let a be a solution to $f(x) \equiv 0 \pmod{p}$. Then by Euclid's Lemma, $p|(a-u)$ or $g(a) \equiv 0 \pmod{p}$. This shows that

$$N_f(p) \leq N_{x-u}(p) + N_g(p) \leq 1 + (n-1) = n,$$

since by induction, $N_g(p)) \leq n-1$ as the degree of $g(x)$ is $n-1$.

This completes the proof of the theorem.

□

REMARK 5.6 The above result is false if p is not a prime. For example the congruence equation

$$x^2 \equiv 1 \pmod{8}$$

has four solutions $x = 1, 3, 5, 7$.

COROLLARY 5.7 If $d|(p-1)$ then the congruence $x^d \equiv 1 \pmod{p}$ has exactly d solutions.

Proof

By previous theorem, the congruence cannot have more than d solutions. For the converse, let $p-1 = de$. Note that

$$x^{p-1} - 1 = (x^d - 1)(x^{d(e-1)} + x^{d(e-2)} + \cdots + x^d + 1).$$

Now,

$$N_{x^{p-1}-1}(p) \leq N_{x^d-1}(p) + N_{x^{d(e-1)}+x^{d(e-2)}+\cdots+1}(p) \leq d + de - d = p - 1.$$

If $N_{x^d-1}(p) < d$, then $N_{x^{p-1}-1}(p) < p-1$. But $N_{x^{p-1}-1}(p) = p-1$ since there are exactly $p-1$ solutions to the equation $x^{p-1} - 1 \equiv 0 \pmod{p}$ by Fermat's little theorem. This contradiction shows that $x^d - 1$ must have exactly d solutions. □

EXAMPLE 5.3 The congruence $x^{10} \equiv 1 \pmod{811}$ has ten solutions and these are

$$1, 212, 241, 311, 339, 472, 500, 570, 599 \quad \text{and} \quad 810.$$

REMARK 5.8 In general, if $d \nmid (p-1)$, the number of solutions for the congruence

$$x^d \equiv 1 \pmod{p}$$

is $(d, p-1)$. This will be shown in the next chapter.

5.4 Wilson's Theorem and Wolstenholme's congruence

THEOREM 5.9 (Wilson) If p is prime then

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof
Let $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. If $p = 2$, then $1 \equiv -1 \pmod{2}$. Let p be an odd prime. Let

$$g(x) = x^{p-1} - [1]_p - (x - [1]_p)(x - [2]_p) \cdots (x - [p-1]_p) \in \mathbf{F}_p[x].$$

The polynomial congruence equation $g(x)$ has at most $p-2$ solutions since the degree of $g(x)$ is $p-2$. But by Fermat's little theorem, the equation $g(x)$ has $p-1$ solutions. Therefore, we conclude that in $g(x)$ must be the zero polynomial in $\mathbf{F}_p[x]$. This implies that

$$x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-(p-1)) \pmod{p}.$$

Setting $x = 0$ we conclude that

$$(p-1)! \equiv -1 \pmod{p}$$

since p is odd. □

Let p is an odd prime. Let

$$F(x) = (x-1)(x-2)\cdots(x-(p-1)).$$

Write

$$F(x) = x^{p-1} - \sigma_1 x^{p-2} + \sigma_2 x^{p-3} - \cdots + \sigma_{p-3}x^2 - \sigma_{p-2}x + \sigma_{p-1},$$

where σ_j denotes the sum of all products of j distinct roots of $F(x)$. In the proof of Theorem 5.9, we have seen that the polynomial

$$f(x) = x^{p-1} - [1]_p - (x - [1]_p)(x - [2]_p)\cdots(x - [p-1]_p)$$

is the zero polynomial in $\mathbf{F}_p[x]$. This means that in $\mathbf{F}_p[x]$,

$$\begin{aligned} x^{p-1} - [1]_p = F(x) &= (x - [1]_p)(x - [2]_p)\cdots(x - [p-1]_p) \\ &= x^{p-1} - [\sigma_1]_p x^{p-2} + [\sigma_2]_p x^{p-3} - \cdots + [\sigma_{p-3}]_p x^2 - [\sigma_{p-2}]_p x + [\sigma_{p-1}]_p. \end{aligned}$$

Comparing the coefficients of x^j on both sides of the above polynomials in $\mathbf{F}_p[x]$, we conclude that

$$\sigma_j \equiv 0 \pmod{p}, 1 \leq j \leq p-2 \tag{5.8}$$

We now prove a result stronger that (5.8) when $j = p-2$.

THEOREM 5.10 (Wolstenholme's congruence) For prime $p \geq 5$,

$$\sigma_{p-2} \equiv 0 \pmod{p^2}.$$

Proof
Let $p \geq 5$ be an odd prime. First, note that

$$F(p) = (p-1)(p-2)\cdots(p-(p-2))(p-(p-1)) = (p-1)!.$$

On the other hand,

$$F(p) = p^{p-1} - \sigma_1 p^{p-2} + \cdots - \sigma_{p-2} p + (p-1)!.$$

This implies that

$$p^{p-2} - \sigma_1 p^{p-3} + \cdots + \sigma_{p-3} p - \sigma_{p-2} = 0. \tag{5.9}$$

By (5.8),

$$\sigma_{p-3} \equiv 0 \pmod{p}$$

and we conclude that

$$\sigma_{p-2} \equiv 0 \pmod{p^2}.$$

□

EXAMPLE 5.4 Let $p \geq 5$ be a prime. Let σ_j be given as follows:

$$\begin{aligned} (x-1)(x-2)\cdots(x-(p-1)) = x^{p-1} &- \sigma_1 x^{p-2} + \sigma_2 x^{p-3} \\ &+ \cdots + (-1)^{p-2}\sigma_{p-2} x + (-1)^{p-1}\sigma_{p-1}. \end{aligned}$$

Show that $\sigma_{p-2} \equiv p\sigma_{p-3} \pmod{p^3}$.

Solution

From (5.9), we find that

$$\sigma_{p-2} = p^{p-2} - \sigma_1 p^{p-3} + \cdots + \sigma_{p-4} p^2 + \sigma_{p-3} p.$$

But σ_j are divisible by p for $j = 1, 2, \cdots p-4$. Therefore, $\sigma_{p-2} \equiv p\sigma_{p-3} \pmod{p^3}$.

6 Primitive roots

6.1 Order of an element in a group

We will need a simple lemma from group theory.

LEMMA 6.1 Let G be a group. If a has order h in G, then a^k has order $h/(h,k)$.

Proof
Let $d = (h,k)$. Let r be the order of a^k. Then $a^{rk} = 1$ and hence $h|rk$. Hence,

$$\frac{h}{d} \Big| \left(r \cdot \frac{k}{d} \right).$$

Since $(h/d, k/d) = 1$, we conclude that $(h/d)|r$.
Next,

$$a^{(h/d)k} = (a^k)^{(h/d)} = 1.$$

Hence, $r|(h/d)$. This implies that

$$r = h/d = h/(h,k).$$

□

6.2 Integers m for which $(\mathbf{Z}/m\mathbf{Z})^*$ is cyclic

DEFINITION 6.1 If g has order $\varphi(m)$ in $(\mathbf{Z}/m\mathbf{Z})^*$ then g is called a primitive root modulo m.

REMARK 6.2 When a primitive root exists for $(\mathbf{Z}/m\mathbf{Z})^*$, we see that $(\mathbf{Z}/m\mathbf{Z})^*$ is a cyclic group of order $\varphi(m)$.

We first turn to the number of primitive roots in $(\mathbf{Z}/m\mathbf{Z})^*$, assuming that $M(m) := (\mathbf{Z}/m\mathbf{Z})^*$ is cyclic.

Let g be a primitive root of $M(m)$. Then every element in $M(m)$ is of the form

g^k. By Lemma 6.1, the order of g^k is $\varphi(m)/(\varphi(m), k)$ and so g^k is a primitive root if and only if $(\varphi(m), k) = 1$. We have thus shown that

THEOREM 6.3 If $M(m)$ is cyclic, then there are precisely $\varphi(\varphi(m))$ primitive roots modulo m.

Our next aim is to show that $M(m)$ is cyclic (or in another words, primitive roots modulo m exists) if and only if $m = 2, 4, p^\alpha$ and $2p^\alpha$, where p is an odd prime and $\alpha \geq 1$. (Note that we do not consider $m = 1$ since $M(1)$ is an empty set.)

We will first establish the fact that if $m = 2, 4, p^\alpha$ and $2p^\alpha$, where p is an odd prime, then $M(m)$ is cyclic.

There is nothing to prove for 2. For $m = 4$ we observe that $[3]_4$ is a primitive root modulo 4.

We now prove that if $m = p$, where p is an odd prime then $M(m)$ is cyclic.

LEMMA 6.4 If n is an integer ≥ 1, then

$$n = \sum_{d|n} \varphi(d).$$

Proof
Observe that

$$\{1, 2, \cdots, n\} = \cup_{d|n} \{\ell | (n, \ell) = d \text{ and } 1 \leq \ell \leq n\}. \tag{6.1}$$

Note that there is a one to one correspondence between the set $A_d = \{\ell | (n, \ell) = d \text{ and } 1 \leq \ell \leq n\}$ and $B_d = \{k | (k, n/d) = 1, 1 \leq k \leq n/d\}$. Since $|B_d| = \varphi(n/d)$, we conclude from (6.1) that

$$n = \sum_{d|n} |A_d| = \sum_{d|n} |B_d| = \sum_{d|n} \varphi(n/d) = \sum_{d|n} \varphi(d).$$

□

THEOREM 6.5 The group $M(p)$ is cyclic.

Proof
Let

$$M(p) = \bigcup_{d|(p-1)} \{y | y \text{ has order } d.\}.$$

Let $f(d) = |\{y | y \text{ has order } d.\}|$.

Suppose $f(d) \neq 0$, then there exists an element of order d. By Corollary 5.7, the elements $Y_d = \{1, y, y^2, \cdots, y^{d-1}\}$ are the only solutions to the congruence equation

$$x^d \equiv 1 \pmod{p}. \tag{6.2}$$

Observe that all elements in $M(p)$ with order d are contained in Y_d since they satisfy (6.2). By Lemma 6.1, the number of elements with order d is $\varphi(d)$ if $f(d) \neq 0$. This means that $f(d) \leq \varphi(d)$. Now,

$$p - 1 = \sum_{d|(p-1)} f(d) \leq \sum_{d|(p-1)} \varphi(d).$$

We have seen that $f(d) \leq \varphi(d)$. If $f(d) = 0$ for some d, then $p-1 < p-1$, which is impossible. Therefore, $f(d) = \varphi(d)$ for all $d|(p-1)$. In particular, $f(p-1) = \varphi(p-1) \neq 0$ and therefore $M(p)$ contains elements with order $p-1$, which implies that $M(p)$ is cyclic. □

We now prove a generalization of Theorem 5.7.

THEOREM 6.6 Let p be a prime number. The number of solutions to

$$x^d \equiv 1 \pmod{p} \tag{6.3}$$

is $(d, p-1)$.

Proof
By Theorem 6.5, $M(p)$ is cyclic. Let g be the generator of $M(p)$. A solution to $x^d \equiv 1 \pmod{p}$ must be of the form g^t for some integer $1 \leq t \leq p-1$. Hence, we may rewrite the congruence equation as

$$g^{td} \equiv 1 \pmod{p}.$$

Since g is the generator of $M(p)$, its order is $p-1$ and by Theorem **??**, we conclude that $p-1|dt$. In other words, t must satisfy $dt \equiv 0 \pmod{p-1}$. By Theorem 1.25, we conclude that the number of t's that satisfy the linear congruence is $(d, p-1)$. This implies that the number of solution to (6.3) is $(d, p-1)$. □

We now give a third proof of Wilson's Theorem using the fact that $M(p)$ is cyclic.

EXAMPLE 6.1 Show that $(p-1)! \equiv -1 \pmod{p}$ using the fact that $M(p)$ is cyclic.

Solution

Let g be a primitive root modulo p. Then

$$(p-1)! \equiv g^{1+2+\cdots+p-1} \equiv g^{p(p-1)/2} \pmod{p}.$$

By Fermat's Little Theorem $g^p \equiv g \pmod{p}$ and thus

$$(p-1)! \equiv g^{(p-1)/2} \pmod{p}.$$

Since $g^{p-1} \equiv 1 \pmod{p}$, we find that $\left(g^{(p-1)/2}\right)^2 \equiv 1 \pmod{p}$. This implies that $g^{(p-1)/2} \equiv 1 \pmod{p}$ or $g^{(p-1)/2} \equiv -1 \pmod{p}$. Since g is a primitive root, $g^{(p-1)/2} \not\equiv 1 \pmod{p}$, and we must have

$$(p-1)! \equiv g^{(p-1)/2} \equiv -1 \pmod{p}.$$

Next, let $\alpha > 1$. We will show that $M(m)$ is cyclic when $m = p^\alpha$, with p an odd prime.

LEMMA 6.7 Let p be an odd prime. There exists a primitive root g modulo p such that

$$g^{p-1} \not\equiv 1 \pmod{p^2}.$$

Proof
Suppose g is a primitive root modulo p such that $g^{p-1} \equiv 1 \pmod{p^2}$. Write

$$g^{p-1} = 1 + p^2 k.$$

Let $h = g + p$. We claim that $h^{p-1} \not\equiv 1 \pmod{p^2}$. Suppose not. Then

$$h^{p-1} \equiv 1 \pmod{p^2}$$

or

$$(g+p)^{p-1} = 1 + p^2 \ell.$$

This gives

$$g^{p-1} + pg^{p-2}(p-1) + g^{p-3}p^2(p-1)(p-2)/2 + \cdots + p^{p-1} = 1 + p^2\ell.$$

But $g^{p-1} = 1 + p^2 k$ and so,

$$1 + p^2 k + pg^{p-2}(p-1) + g^{p-3}p^2(p-1)(p-2)/2 + \cdots + p^{p-1} = 1 + p^2\ell$$

and this implies that $p^2 | p(p-1)g^{p-2}$, or $p | g^{p-2}$, which is a contradiction. Hence, $h^{p-1} \not\equiv 1 \pmod{p^2}$. □

LEMMA 6.8 Let g be a primitive root modulo p such that

$$g^{p-1} \not\equiv 1 \pmod{p^2}.$$

Then for every $\alpha \geq 3$, we have

$$g^{\varphi(p^{\alpha-1})} \not\equiv 1 \pmod{p^\alpha}.$$

Proof
We first proved the case $\alpha = 3$. Since g is a primitive root modulo p such that

$$g^{p-1} \not\equiv 1 \pmod{p^2}.$$

Then since $g^{p-1} \equiv 1 \pmod{p}$, we deduce that

$$g^{p-1} = 1 + sp$$

where $p \nmid s$. Next, suppose $g^{\varphi(p^2)} \equiv 1 \pmod{p^3}$ then $g^{p(p-1)} = 1 + p^3 t$. This implies that

$$1 + p^3 t = g^{(p-1)p} = (1 + sp)^p = 1 + sp^2 + \frac{p(p-1)}{2}(sp)^2 + \cdots + (sp)^p.$$

This implies that $p|s$, which is a contradiction. Therefore, $g^{\varphi(p^2)} \not\equiv 1 \pmod{p^3}$.
We now prove the result for $\alpha \geq 3$ by induction. Suppose

$$g^{\varphi(p^{\alpha-2})} \not\equiv 1 \pmod{p^{\alpha-1}}. \tag{6.4}$$

We want to show that

$$g^{\varphi(p^{\alpha-1})} \not\equiv 1 \pmod{p^{\alpha}}.$$

By Euler's Theorem,

$$g^{\varphi(p^{\alpha-2})} \equiv 1 \pmod{p^{\alpha-2}}$$

and hence,

$$g^{\varphi(p^{\alpha-2})} = 1 + sp^{\alpha-2},$$

for some integer s. By (6.4), we conclude that $p \nmid s$. Suppose

$$g^{\varphi(p^{\alpha-1})} \equiv 1 \pmod{p^{\alpha}},$$

or $g^{\varphi(p^{\alpha-1})} = 1 + p^{\alpha}k$. Then

$$(1 + sp^{\alpha-2})^p = g^{p\varphi(p^{\alpha-2})} = g^{\varphi(p^{\alpha-1})} = 1 + p^{\alpha}k.$$

This yields

$$1 + sp^{\alpha-2}p + s^2 p^{2(\alpha-2)} p(p-1)/2 + \cdots + (sp)^{p(\alpha-2)} = 1 + p^{\alpha}k.$$

(Note that $2\alpha - 4 + 1 \geq \alpha$ since $\alpha \geq 3$.) Therefore, p^{α} divides $p^{\alpha-1}s$, which implies that $p|s$, a contradiction. Hence,

$$g^{\varphi(p^{\alpha-1})} \not\equiv 1 \pmod{p^{\alpha}}.$$

□

THEOREM 6.9 The group $M(p^{\alpha})$ is cyclic.

Proof

From Lemma 6.8, we know that there exists a primitive g modulo p such that

$$g^{\varphi(p^{\alpha-1})} \not\equiv 1 \pmod{p^{\alpha}}.$$

We will show that the order of this element is $\varphi(p^{\alpha})$. Let ℓ be the order of $g^{\varphi(p^{\alpha-1})}$. By Euler's Theorem,

$$\left(g^{\varphi(p^{\alpha-1})}\right)^{p} \equiv g^{\varphi(p^{\alpha})} \equiv 1 \pmod{p^{\alpha}}$$

since

$$\varphi(p^{\alpha}) = p\varphi(p^{\alpha-1}).$$

Hence $\ell | p$ and $\ell = p$ since $\ell \neq 1$. Let k be the order of g. Then by Lemma 6.1, the order of $g^{\varphi(p^{\alpha-1})}$ is

$$\frac{k}{(\varphi(p^{\alpha-1}), k)} = \ell = p.$$

This implies that

$$k = p\left(\varphi(p^{\alpha-1}), k\right) = (\varphi(p^{\alpha}), kp)$$

or

$$1 = \left(\frac{p^{\alpha-1}(p-1)}{k}, p\right).$$

In other words,

$$k = p^{\alpha-1}d$$

for some $d|(p-1)$. Now,

$$g^{p^{\alpha-1}d} \equiv g^{k} \equiv 1 \pmod{p^{\alpha}}$$

implies that

$$g^{p^{\alpha-1}d} \equiv 1 \pmod{p}$$

and this shows that

$$g^{d} \equiv 1 \pmod{p}$$

since $g^{p} \equiv g \pmod{p}$. Since g is a primitive root modulo p, $(p-1)|d$. Therefore,

$$k = p^{\alpha-1}d = p^{\alpha-1}(p-1) = \varphi(p^{\alpha})$$

and this shows that g is a primitive root modulo p^{α}. □

Since

$$M(2p^{\alpha}) \simeq M(p^{\alpha}),$$

we conclude that $M(2p^{\alpha})$ is also cyclic.

We have thus shown that

THEOREM 6.10 Let p be an odd prime. The group $M(m)$ is cyclic if

$$m = 2, 4, p^{\alpha} \quad \text{and} \quad 2p^{\alpha}.$$

EXAMPLE 6.2 Prove that 3 is a primitive root of all integers of the form 7^k.

Solution

We check that 3 is a primitive root modulo 7 and $3^6 \equiv 43 \not\equiv 1 \pmod{7^2}$. Therefore, 3 is a primitive root modulo 7^k for any positive integer k.

EXAMPLE 6.3 Show that if r is a primitive root modulo p^2, then r is a primitive root modulo p.

Solution

Suppose r is not a primitive root modulo p. Let $d|(p-1)$ and $d < p-1$ be the order of r. Then $r^d = 1+sp$ and $r^{dp} = 1+sp^2+s^2p^2p(p-1)/2+\cdots \equiv 1 \pmod{p^2}$. But the order of r modulo p^2 is $p(p-1)$ since r is a primitive root modulo p^2. Hence $p(p-1)|pd$ or $(p-1)|d$. This implies that $d \geq p-1$ and contradicts our assumption about d being less than $p-1$.

6.3 Integers m for which $(\mathbf{Z}/m\mathbf{Z})^*$ is not cyclic

We will now prove that $M(m)$ is not cyclic for $m \neq 1, 2, 4, p^{\alpha}$ and $2p^{\alpha}$.

We first prove that $M(2^{\beta})$ is not cyclic for $\beta \geq 3$. This follows from the following lemma:

LEMMA 6.11 If $\beta \geq 3$ then $M(2^{\beta})$ is not cyclic.

Proof

The elements in $M(2^{\beta})$ are of the form $[x]_{2^{\beta}}$, with x being an odd integer. If we can show that all elements of $M(2^{\beta})$ has order strictly less than $2^{\beta-1}$, then we can conclude that $M(2^{\beta})$ is not cyclic. Hence it suffices to show that for all odd integers x,

$$x^{2^{\beta-2}} \equiv 1 \pmod{2^{\beta}}. \tag{6.5}$$

When $\beta = 3$ then $x^2 \equiv 1 \pmod 8$ for all odd integers x. This can be verified directly. We now prove by induction that $M(2^{\beta})$ is not cyclic for all positive

integer $\beta \geq 3$. Suppose (6.5) is true for positive integers less than β. Then this means that

$$x^{2^{\beta-3}} \equiv 1 \pmod{2^{\beta-1}}$$

for all odd integers x. Therefore,

$$x^{2^{\beta-3}} = 1 + 2^{\beta-1}t.$$

Squaring both sides of the above, we find that

$$x^{2^{\beta-2}} = 1 + 2^{\beta}t'.$$

Hence,

$$x^{2^{\beta-2}} \equiv 1 \pmod{2^{\beta}},$$

and this completes our proof that $M(2^{\beta})$ is not cyclic. □

Next, we observe that if m is not a prime or power of a prime, then m can be expressed in the form ab with $(a, b) = 1$ and $1 < a < b$. Note that $M(ab)$ is isomorphic to $M(a) \times M(b)$. Since $[-1]_a^2 = [1]_a$, we conclude that if $a \neq 2$, then $M(a)$ contains an element of order 2. Similarly $M(b)$ contains an element of order 2. By Chinese Remainder Theorem, there exists elements $[\alpha]_{ab}$ and $[\beta]_{ab}$ in $M(ab)$ satisfying

$$\alpha \equiv -1 \pmod{a}, \alpha \equiv 1 \pmod{b}$$

and

$$\beta \equiv 1 \pmod{a}, \beta \equiv -1 \pmod{b}.$$

Note that

$$\alpha^2 \equiv \beta^2 \equiv 1 \pmod{p} \text{ and } \alpha \not\equiv \beta \pmod{p}.$$

This implies that $M(ab)$ contains more than one element of order 2 and we conclude that $M(ab)$ cannot be cyclic. This implies that if m is not a prime, a prime power or $2p^{\alpha}$, with p an odd prime, then $M(m)$ is not cyclic.

This completes our proof that $M(m)$ is not cyclic if $m \neq 2, 4, p^{\alpha}$ and $2p^{\alpha}$.

7 Quadratic Reciprocity Law

7.1 Primitive roots and solutions of congruences

In general, given a positive integer N, there is no simple way to determine if

$$x^d \equiv a \pmod{N}$$

is solvable or not. However, in the case when $M(N)$ is cyclic, we have the following theorem:

THEOREM 7.1 Suppose $m = 1, 2, 4, p^\alpha$ or $2p^\alpha$, where p is an odd prime. Let $(a, m) = 1$ and let $d = (\varphi(m), n)$. The congruence

$$x^n \equiv a \pmod{m} \tag{7.1}$$

is solvable if and only if

$$a^{\varphi(m)/d} \equiv 1 \pmod{m}.$$

Proof

We may assume that $n \leq \varphi(m)$ by Euler's Theorem. Let g be a primitive root modulo m. If

$$x^n \equiv a \pmod{m}$$

has a solution, then let g^t be one of its solution. Let $a \equiv g^s$ for some integer s. Then $g^{tn} \equiv g^s \pmod{m}$ which implies that $tn \equiv s \pmod{\varphi(m)}$. Since the above congruence is solvable, it means that $(n, \varphi(m)) = d$ divides s. Let $s = dk$. This implies that

$$a^{\varphi(m)/d} \equiv g^{dk\varphi(m)/d} \equiv g^{k\varphi(m)} \equiv 1 \pmod{m}.$$

Conversely, suppose

$$a^{\varphi(m)/d} \equiv 1 \pmod{m}.$$

Let $a = g^s$. Note that from our assumption and the fact that g is a primitive root, we must have

$$\varphi(m) | (s\varphi(m)/d).$$

Hence $d|s$, or $s = dk$.

Now consider the linear congruence

$$nt \equiv s \pmod{\varphi(m)}.$$

Note that since $d = (n, \varphi(m))$ divides $s = dk$, the above congruence is solvable by Theorem 1.25. We may write $nt = s + \varphi(m)h$. Now, let $u = g^t$. Then

$$u^n = g^{nt} \equiv g^{s+\varphi(m)h} \equiv g^s \equiv a \pmod{m}$$

and hence

$$x^n \equiv a \pmod{m}$$

is solvable. □

By specifying $n = 2$ and $m = p$ we see that

THEOREM 7.2 (Euler's Criterion) The congruence equation

$$x^2 \equiv a \pmod{p}$$

is solvable if and only if

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

7.2 The Legendre Symbol

Let a be any integer relatively prime to p, where p is an odd prime. The Legendre symbol is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } x^2 \equiv a \pmod{p} \text{ is solvable,} \\ -1 & \text{otherwise.} \end{cases}$$

When $p|a$, we set

$$\left(\frac{a}{p}\right) = 0.$$

From the Euler Criterion, we see immediately that if $p \nmid a$,

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

This is because $a^{p-1} \equiv 1 \pmod{p}$ and so $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$.

EXAMPLE 7.1 Let p be an odd prime. Show that the Legendre symbol $\left(\frac{n}{p}\right)$ is a completely multiplicative function.

Solution

From Euler's Criterion, we obtain immediately that if $(mn, p) = 1$, then

$$\left(\frac{mn}{p}\right) \equiv (mn)^{(p-1)/2} \equiv m^{(p-1)/2} n^{(p-1)/2} \equiv \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) \pmod{p}.$$

This implies that

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right).$$

When $(mn, p) = p$, then $p|m$ or $p|n$ and

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) = 0.$$

This implies that the Legendre symbol $\left(\frac{n}{p}\right)$ is a completely multiplicative function.

EXAMPLE 7.2 Let p be an odd prime. Suppose that $a = bp + r$. Show that

$$\left(\frac{a}{p}\right) = \left(\frac{r}{p}\right).$$

Solution

Note that solving

$$x^2 \equiv a \pmod{p}$$

is the same as solving

$$x^2 \equiv bp + r \equiv r \pmod{p}.$$

This means that the first congruence is solvable if and only if the second congruence is solvable. Therefore,

$$\left(\frac{a}{p}\right) = \left(\frac{r}{p}\right).$$

In the subsequent sections, we will learn an algorithm in computing the Legendre symbol, thereby allowing us to determine the solvability of the congruence

$$x^2 \equiv a \pmod{p}.$$

DEFINITION 7.1 For $(a, p) = 1$, we say that a is a quadratic residue modulo p if $x^2 \equiv a \pmod{p}$ is solvable. Otherwise, we say that a is a quadratic non-residue modulo p.

7.3 Gauss Lemma

In this section, we give a proof of the Gauss Lemma. For the following proof, let $\ell_p(a)$ be the least non-negative residue of a modulo p.

THEOREM 7.3 Let p be a prime and let a be an integer such that $(a, p) = 1$. Consider

$$U := \{1, 2, \cdots, \frac{p-1}{2}\}$$

and let

$$V := \{\ell_p(au) | u \in U\}.$$

Suppose there are m elements in V which are greater than $p/2$, then

$$\left(\frac{a}{p}\right) = (-1)^m.$$

Proof
Let $V = R \cup T$, where R contains integers in U and T contains integers greater than $p/2$. Let $T' = \{p - t | t \in T\}$. Note that T' is a subset of U. We claim that $U = R \cup T'$.

First, all elements in R are distinct elements of U. This is because if

$$r \equiv r' \pmod{p}$$

for $r, r' \in R$, then since $r \equiv au \pmod{p}$ and $r \equiv au' \pmod{p}$ for some $u, u' \in A$. This implies that $u \equiv u' \pmod{p}$ and $r = r'$. Similarly, if $p - t \equiv p - t' \pmod{p}$, we must have $t = t'$. Suppose $r \equiv p - t \pmod{p}$. Then $r + t \equiv 0 \pmod{p}$. But $r \equiv au \pmod{p}$ and $t \equiv au' \pmod{p}$ for some $u, u' \in U$. This implies that $u + u' \equiv 0 \pmod{p}$ which is impossible since u, u' are both less than $p/2$. Therefore, R and T' contains distinct integers less than $(p-1)/2$. Since there are $(p-1)/2$ such integers in $R \cup T'$, we conclude that $U = R \cup T'$.

Taking product of all the elements on the left hand side and right hand side, we conclude that

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &\equiv \prod_{r \in R} r \prod_{t \in T} (p - t) \equiv (-1)^{|T|} \prod_{r \in R} r \prod_{t \in T} t \\ &\equiv (-1)^{|T|} a^{(p-1)/2} \left(\frac{p-1}{2}\right)! \pmod{p}.\end{aligned}$$

Therefore,

$$a^{(p-1)/2} \equiv (-1)^{|T|} \pmod{p},$$

and hence,

$$\left(\frac{a}{p}\right) = (-1)^{|T|}.$$

□

7.4 Proofs of Gauss' Quadratic Reciprocity Law

Let $a = -1$ then $m = (p-1)/2$ since $\ell_p(au) \notin U$ for all $u \in U$. From Euler's Criterion or Gauss Lemma (Theorem 7.3), we deduce that

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

This is the first part of Gauss' quadratic reciprocity law.

Let $a = 2$ and $p \equiv 1 \pmod 4$. Set $p = 4\ell + 1$. We have $U = \{2, 4, \cdots, 2\ell, 2\ell + 2, \cdots, 4\ell\}$. Hence $m = \ell$. In other words,

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p = 8\ell + 1 \\ -1 & \text{if } p = 8\ell + 5. \end{cases}$$

Similarly, we have

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p = 8\ell + 7 \\ -1 & \text{if } p = 8\ell + 3. \end{cases}$$

In short, we may write

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

We now prove the final part of Gauss' quadratic reciprocity law.

We first prove a lemma.

LEMMA 7.4 For any real number x, the function $[x]$ is the greatest integer less than or equal to x. For any distinct odd primes p and q,

$$\left(\frac{q}{p}\right) = (-1)^t,$$

where

$$t = \sum_{j=1}^{(p-1)/2} \left[\frac{qj}{p}\right] = \sum_{1 \le j < \frac{p}{2}} \left[\frac{qj}{p}\right].$$

Proof

First, we note that for $1 \le j \le (p-1)/2$, we can write using the division algorithm that

$$qj = h_j p + k_j, 1 \le k_j \le (p-1),$$

where

$$h_j = \left[\frac{qj}{p}\right].$$

Note that k_j is either greater that $p/2$ or less than $p/2$. Let m be the number of j's for which c_j exceeds $(p-1)/2$. We have encountered this number in Gauss Lemma. Now, if k_j is less than $p/2$ we leave it as k_j and if it is greater than $p/2$, we write $k_j = p - \ell_j$ with ℓ_j less than $p/2$. Hence,

$$\begin{aligned}\sum_{j=1}^{(p-1)/2} jq &= p\sum_{j=1}^{(p-1)/2} h_j + \sum_{\substack{1\le u\le (p-1)/2\\ k_u > p/2}} (p-\ell_u) + \sum_{\substack{1\le v\le (p-1)/2\\ k_v < p/2}} k_v \\ &= p\sum_{j=1}^{(p-1)/2} h_j + pm - 2\sum_{\substack{1\le j\le (p-1)/2\\ k_j > p/2}} \ell_j + \sum_u \ell_u + \sum_v k_v.\end{aligned}$$

But in the proof of Gauss Lemma, we have shown that

$$\sum_u \ell_u + \sum_v k_v = \sum_{j=1}^{(p-1)/2} j.$$

Therefore, we conclude that

$$(q-1)\left(\sum_{j=1}^{(p-1)/2} j\right) = p\sum_{j=1}^{(p-1)/2} h_j + pm - 2\sum_{\substack{1\le j\le (p-1)/2\\ k_j > p/2}} \ell_j.$$

The left hand side is even and so is the last term on the right hand side. Hence

$$(-1)^{pt} = (-1)^{pm}$$

or

$$(-1)^t = (-1)^m = \left(\frac{q}{p}\right)$$

where the last equality follows from Gauss Lemma.

□

We next derive a simple lemma.

LEMMA 7.5 Suppose p and q are distinct odd primes. Then

$$\sum_{j=1}^{(p-1)/2} \left[\frac{qj}{p}\right] + \sum_{\ell=1}^{(q-1)/2} \left[\frac{p\ell}{q}\right] = \frac{(p-1)(q-1)}{4}.$$

Proof
Write

$$\sum_{j=1}^{(p-1)/2}\left[\frac{qj}{p}\right]=\sum_{j=1}^{(p-1)/2}\sum_{1\le\ell\le\frac{qj}{p}}1=\sum_{1\le\ell<\frac{q}{2}}\sum_{\frac{p\ell}{q}\le j<\frac{p}{2}}1.$$

The upper bound for j is obtained by observing that

$$\ell<\frac{qj}{p}<\frac{q}{p}\cdot\frac{p}{2}<q/2$$

and that $\ell<\frac{qj}{p}$ implies that $j>\frac{\ell p}{q}$. Therefore,

$$\sum_{j=1}^{(p-1)/2}\left[\frac{qj}{p}\right]=\sum_{1\le\ell\le\frac{q-1}{2}}\sum_{1\le j\le\frac{p-1}{2}}1-\sum_{1\le\ell\le\frac{q-1}{2}}\sum_{1\le j<p\frac{\ell}{q}}1=\frac{q-1}{2}\frac{p-1}{2}-\sum_{\ell=1}^{(q-1)/2}\left[\frac{p\ell}{q}\right],$$

which gives the desired identity. □

The final part of Gauss' Quadratic Reciprocity Law now follows by observing that

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\sum_{j=1}^{(p-1)/2}\left[\frac{qj}{p}\right]+\sum_{\ell=1}^{(q-1)/2}\left[\frac{p\ell}{q}\right]}=(-1)^{(p-1)(q-1)/4}.$$

We have thus completed the proof of the quadratic reciprocity law and we summarize the result as follow:

THEOREM 7.6 Let p and q be distinct primes. Then we have

$$\left(\frac{-1}{p}\right)=(-1)^{(p-1)/2}$$
$$\left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}$$
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{(p-1)(q-1)/4}.$$

EXAMPLE 7.3 Show that $x^2\equiv 10 \pmod{89}$ is solvable.

Solution

We compute

$$\left(\frac{10}{89}\right)=\left(\frac{2}{89}\right)\left(\frac{5}{89}\right)=(-1)^{(89^2-1)/8}\left(\frac{5}{89}\right)=\left(\frac{89}{5}\right)=1.$$

7.5 The Jacobi Symbol

In this section, we discuss an extension of the Legendre symbol.

DEFINITION 7.2 Let Q be a positive odd integer so that

$$Q = q_1 q_2 \cdots q_s$$

where q_i are not necessarily distinct. The Jacobi symbol is defined by

$$\left(\frac{P}{Q}\right) = \prod_{j=1}^{s} \left(\frac{P}{q_j}\right)$$

where the expressions on the right hand side involving q_j are the Legendre symbols.

We observe that if Q is prime then the Jacobi symbol is simply the Legendre symbol. We also note that if $(P, Q) > 1$, then

$$\left(\frac{P}{q_j}\right) = 0$$

for some j and hence

$$\left(\frac{P}{Q}\right) = 0.$$

Now if P is a quadratic residue modulo Q, then

$$x^2 \equiv P \pmod{q_j}$$

is solvable and hence

$$\left(\frac{P}{Q}\right) = 1.$$

The converse, however, is not true. Although

$$\left(\frac{2}{15}\right) = 1,$$

the congruence

$$x^2 \equiv 2 \pmod{15}$$

is not solvable.

From the definition of the Jacobi symbol and the properties of the Legendre

symbol, it is immediate that

$$\left(\frac{P}{Q}\right)\left(\frac{P}{Q'}\right) = \left(\frac{P}{QQ'}\right)$$
$$\left(\frac{P}{Q}\right)\left(\frac{P'}{Q}\right) = \left(\frac{PP'}{Q}\right)$$
$$\left(\frac{P^2}{Q}\right) = 1 \quad \text{and} \quad \left(\frac{P}{Q^2}\right) = 1$$

Finally, we observe that if $P \equiv P' \pmod{Q}$, then

$$\left(\frac{P}{Q}\right) = \left(\frac{P'}{Q}\right).$$

The main result we want to show in this section is

THEOREM 7.7 If Q is odd positive integer, then

$$\left(\frac{-1}{Q}\right) = (-1)^{\frac{Q-1}{2}}$$
$$\left(\frac{2}{Q}\right) = (-1)^{\frac{Q^2-1)}{8}}$$
$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}.$$

Proof
To prove the first equality, we observe that

$$\frac{ab-1}{2} - \left(\frac{a-1}{2} + \frac{b-1}{2}\right) = \frac{(a-1)(b-1)}{2}.$$

The numerator of the right hand side is divisible by 4 if both a and b are odd. Hence,

$$\frac{ab-1}{2} \equiv \left(\frac{a-1}{2} + \frac{b-1}{2}\right) \pmod{2}.$$

Hence if $Q = q_1 q_2 \cdots q_s$, then

$$\sum_{j=1}^{s}\left(\frac{q_j-1}{2}\right) \equiv \frac{Q-1}{2} \pmod{2}.$$

This implies that

$$\left(\frac{-1}{Q}\right) = \prod_{j=1}^{s}\left(\frac{-1}{q_j}\right) = (-1)^{\sum_{j=1}^{s}(q_j-1)/2} = (-1)^{\frac{Q-1}{2}}.$$

The proof of the second equality is similar except that we used the relation

$$\frac{a^2b^2-1}{8} - \left(\frac{a^2-1}{8} + \frac{b^2-1}{8}\right) = \frac{(a^2-1)(b^2-1)}{8}$$

and observe that the numerator of the right hand side is divisible by 64.

The proof of the last equality follows in exactly the same way as the proof of the first equality. More precisely, we write

$$P = \prod_{j=1}^{s} p_j \text{ and } Q = \prod_{\ell=1}^{t} q_\ell$$

and observe that

$$\begin{aligned}\left(\frac{P}{Q}\right) &= \prod_{j=1}^{s}\prod_{\ell=1}^{t}\left(\frac{p_j}{q_\ell}\right)\\ &= \prod_{j=1}^{s}\left(\frac{Q}{p_j}\right)(-1)^{\frac{p_j-1}{2}\cdot\sum_{\ell=1}^{t}\frac{q_\ell-1}{2}}\\ &= \prod_{j=1}^{s}\left(\frac{Q}{p_j}\right)(-1)^{\frac{p_j-1}{2}\cdot\frac{Q-1}{2}}\\ &= \left(\frac{Q}{P}\right)(-1)^{\frac{(P-1)(Q-1)}{4}}.\end{aligned}$$

□

With the Jacobi symbol, we can now calculate Legendre symbol without having to factorize integers (except for factoring -1 and 2).

7.6 Appendix

In this section, we will give another proof of Gauss' Laws of Quadratic Reciprocity. This proof is due to G. Eisenstein and can be found in J.P. Serre's "A course in Arithmetic". First, we need a lemma.

LEMMA 7.8 For odd positive integer m, we have

$$\frac{\sin mx}{\sin x} = (2i)^{(m-1)} \prod_{1\le j\le (m-1)/2}\left(\sin^2 x - \sin^2\frac{2\pi j}{m}\right). \tag{7.2}$$

Proof
Let $U = \{1, \zeta_m, \zeta_m^2, \cdots, \zeta_m^{m-1}\}$, where $\zeta_m = e^{2\pi i/m}$, where m is odd. This is a cyclic group of order m generated by ζ_m. Note that since $(2, m) = 1$, the group is also generated by ζ_m^2 and we have $\{1, \zeta_m^2, \cdots, \zeta_m^{2(m-1)}\} = U$. Next, we know that

$$z^m - 1 = (z-1)\prod_{j=1}^{m-1}(z - e^{2\pi ij/m}) = (z-1)\prod_{j=1}^{m-1}(z - e^{4\pi ij/m}).$$

Let $z = e^{2ix}$. Then

$$e^{imx}(e^{imx} - e^{-imx}) = e^{ix}(e^{ix} - e^{-ix}) \prod_{j=1}^{m-1} e^{ix+2\pi ij/m}(e^{ix-2\pi ij/m} - e^{-ix+2\pi ij/m}).$$

This yields

$$2ie^{imx} \sin mx = 2ie^{ix} \sin x \times e^{i(m-1)x} e^{(2\pi i/m)(m-1)m/2} \prod_{j=1}^{m-1} (2i) \sin(x - 2\pi j/m).$$

Hence, by expressing $(m+1)/2 \leq j \leq m-1$ as $m-k, 1 \leq k \leq (m-1)/2$, we find that

$$\begin{aligned}
\sin mx &= (2i)^{m-1} \sin x \prod_{j=1}^{(m-1)/2} \sin(x - 2\pi j/m) \sin(x - 2\pi(m-j)/m) \\
&= (2i)^{m-1} \sin x \prod_{j=1}^{(m-1)/2} \sin(x - 2\pi j/m) \sin(x + 2\pi j/m) \\
&= (2i)^{m-1} \sin x \prod_{j=1}^{(m-1)/2} (\sin x - \sin 2\pi j/m)(\sin x + \sin 2\pi j/m) \\
&= (2i)^{m-1} \sin x \prod_{j=1}^{(m-1)/2} (\sin^2 x - \sin^2 2\pi j/m),
\end{aligned}$$

where we have used the identity $\sin(a+b)\sin(a-b) = (\sin a + \sin b)(\sin a - \sin b)$ in the second equality. This completes the proof of the Lemma.

□

The main part of Gauss' quadratic reciprocity law states that for odd distinct primes p, q

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

Let $U = \{1, 2, \cdots, (p-1)/2\}$. Let

$$e_q(u) = \begin{cases} 1 & \text{if } \ell_p(qu) \in U \\ -1 & \text{if } \ell_p(qu) \notin U. \end{cases}.$$

Note that $u_q = \ell_p(e_q(u)qu) \in U$ and $U = \{u_q | u \in U\}$. Now, define

$$F([a]_p) = \sin \frac{2\pi a}{p}.$$

Using the above notation, we find that $[qu]_p = [e_q(u)u_q]_p$ and

$$F([qu]_p) = \sin \frac{2\pi}{p} qu = e_q(u) \sin \frac{2\pi}{p} u_q.$$

Next, note that $e_q(u) = -1$ precisely when $\ell_p(qu)$ exceeds $p/2$. Therefore, by Gauss' Lemma,

$$\left(\frac{q}{p}\right) = \prod_{u\in U} e_q(u) = \prod_{u\in U} \frac{\sin\dfrac{2\pi}{p}qu}{\sin\dfrac{2\pi}{p}u_q} = \prod_{u\in U} \frac{\sin\dfrac{2\pi}{p}qu}{\sin\dfrac{2\pi}{p}u}.$$

Applying Lemma 7.8, we deduce that

$$\left(\frac{q}{p}\right) = \prod_{u\in U} (2i)^{q-1} \prod_{v\in V} \left(\sin^2\frac{2\pi u}{p} - \sin^2\frac{2\pi v}{q}\right),$$

where $V = \{1, 2, \cdots, (q-1)/2\}$. Hence

$$\left(\frac{q}{p}\right) = (2i)^{(q-1)(p-1)/2} \prod_{u\in U}\prod_{v\in V} \left(\sin^2\frac{2\pi u}{p} - \sin^2\frac{2\pi v}{q}\right).$$

Interchanging the role of p and q, we deduce that

$$\left(\frac{p}{q}\right) = (2i)^{(p-1)(q-1)/2} \prod_{v\in V}\prod_{u\in U} \left(\sin^2\frac{2\pi v}{q} - \sin^2\frac{2\pi u}{p}\right).$$

Using the last two identities, we conclude that

$$\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{q}{p}\right).$$

8 Jacobsthal sums and primes of the form $x^2 + y^2$

8.1 Two sums involving Legendre Symbol

In Theorem 1.31, we prove that if $p \equiv 1 \pmod 4$ then $p = x^2 + y^2$ for some integers x and y using Wilson's Theorem and Fermat's method of descent. The proof given in Chapter 1 gives only the existence of positive integers x and y satisfying $p = x^2 + y^2$. In this chapter, we will learn a second proof of Theorem 1.31 with the help of Legendre symbol. Theorem 1.31 will be proved by constructing explicitly integers x and y such that $p = x^2 + y^2$. This section is adapted from "Number Theory" pp. 135–138, by G.E. Andrews.

We first need two lemmas.

LEMMA 8.1 Let p be an odd prime. We have

$$\sum_{m (\mathrm{mod}\ p)} \left(\frac{m}{p}\right) = 0,$$

where $\sum_{m\ (\mathrm{mod}\ p)}$ denote the sum over any complete set of residues modulo p.

We will give two proofs of the above lemma.

Proof

Note that using primitive roots modulo p, we see that if g is a primitive root modulo p, then the even powers of g are quadratic residues and the odd powers of g are quadratic non-residues. This follows from the fact that since g is a primitive root,

$$g^{(p-1)/2} \equiv -1 \pmod p$$

and hence, $\left(\frac{g}{p}\right) = -1$. Therefore, there are $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic non-residues. Therefore in the sum

$$\sum_{m (\mathrm{mod}\ p)} \left(\frac{m}{p}\right),$$

there are $(p-1)/2$ terms which take the value 1 and $(p-1)/2$ terms which take the value -1. In other words,

$$\sum_{m \pmod p} \left(\frac{m}{p}\right) = 0.$$

This completes the first proof of Lemma 8.1.

We begin the second proof by recalling that if g is a primitive root modulo p then $\left(\frac{g}{p}\right) = -1$. Observe that

$$\sum_{m \pmod p} \left(\frac{m}{p}\right) = \sum_{m \pmod p} \left(\frac{gm}{p}\right) = \left(\frac{g}{p}\right) \sum_{m \pmod p} \left(\frac{m}{p}\right).$$

Since $\left(\frac{g}{p}\right) = -1$, we conclude that

$$\sum_{m \pmod p} \left(\frac{m}{p}\right) = 0,$$

and we complete the second proof of Lemma 8.1.

□

LEMMA 8.2 Let p be an odd prime. We have

$$\sum_{m \pmod p} \left(\frac{(m-a)(m-b)}{p}\right) = \begin{cases} p-1 & \text{if } a \equiv b \pmod p \\ -1 & \text{if } a \not\equiv b \pmod p. \end{cases}$$

Proof

If $a \equiv b \pmod p$, then

$$\sum_{m \pmod p} \left(\frac{(m-a)(m-b)}{p}\right) = \sum_{m \pmod p} \left(\frac{(m-a)(m-a)}{p}\right) = p-1,$$

as there are $p-1$ 1's in the sum since $\left(\frac{m-a}{p}\right) = 0$ when $m = a$.

Next, replace m by $m+a$, we find that

$$\begin{aligned} \sum_{m \pmod p} \left(\frac{(m-a)(m-b)}{p}\right) &= \sum_{m \pmod p} \left(\frac{m(m-(b-a))}{p}\right) \\ &= \sum_{\substack{m \pmod p \\ m \not\equiv 0 \pmod p}} \left(\frac{m(m-(b-a))}{p}\right) \end{aligned}$$

since $\left(\frac{m}{p}\right) = 0$ when $p|m$. Let m^{-1} denote the integer ℓ satisfying

$$m\ell \equiv 1 \pmod p.$$

Then

$$\begin{aligned}\sum_{\substack{m \pmod p \\ m \not\equiv 0 \pmod p}} \left(\frac{m(m-(b-a))}{p}\right) &= \sum_{\substack{m \pmod p \\ m \not\equiv 0 \pmod p}} \left(\frac{(m^2}{p}\right)\left(\frac{1-(b-a)m^{-1}}{p}\right) \\ &= \sum_{m^{-1} \pmod p} \left(\frac{1-m^{-1}(b-a)}{p}\right) - 1 \\ &= -1\end{aligned}$$

by Lemma 8.1. Note that number -1 in the second last line is added so that we could sum over complete residues $m^{-1} \pmod p$. We also observe that summing over m from 1 to $p-1$ is equivalent to summing over m^{-1} from 1 to $p-1$ since taking inverses of elements in $M(p)$ is a bijection. □

8.2 The Jacobsthal identity and primes of the form $x^2 + y^2$

We are now ready to state and prove the following identity of Jacobsthal.

THEOREM 8.3 Let $p \equiv 1 \pmod 4$ be a prime. If ℓ is a quadratic non-residue modulo p, then

$$\left(\frac{1}{2}\sum_{n=1}^{p}\left(\frac{n(n^2-1)}{p}\right)\right)^2 + \left(\frac{1}{2}\sum_{n=1}^{p}\left(\frac{n(n^2-\ell)}{p}\right)\right)^2 = p.$$

Proof

Let

$$S(m) = \sum_{n=1}^{p}\left(\frac{n(n^2-m)}{p}\right).$$

Note that $S(0) = 0$ by Lemma 8.1 and $S(m+Np) = S(m)$ for any integer N.

Let $k \not\equiv 0 \pmod p$. Then

$$\begin{aligned}S(m) &= \sum_{n \pmod p}\left(\frac{k^4}{p}\right)\left(\frac{n(n^2-m)}{p}\right) \\ &= \sum_{n \pmod p}\left(\frac{k^2n}{p}\right)\left(\frac{k^2n^2-k^2m}{p}\right) \\ &= \left(\frac{k}{p}\right)\sum_{n \pmod p}\left(\frac{kn}{p}\right)\left(\frac{(kn)^2-k^2m}{p}\right) \\ &= \left(\frac{k}{p}\right)S(k^2m).\end{aligned}$$

Hence, we have

$$S^2(k^2 m) = S^2(m). \tag{8.1}$$

If u is a quadratic residue modulo p, then $u \equiv k^2 \pmod{p}$ for some integer k and

$$S^2(u) = S^2(k^2 \cdot 1) = S^2(1) \tag{8.2}$$

by setting $m = 1$ in (8.1).

If v is a non-residue, then $v = g^{2\ell+1}$ where g is a fixed primitive root modulo p. This is because all quadratic non-residues are odd powers of primitive roots modulo p. Then by (8.1),

$$S^2(v) = S^2(gg^{2\ell}) = S^2(g). \tag{8.3}$$

We note that we can replace g by any quadratic non-residue modulo p.

There are $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic non-residues and hence by (8.2) and (8.3), we deduce that

$$\sum_{m(\text{mod } p)} S^2(m) = S^2(0) + \frac{p-1}{2}\left(S^2(1) + S^2(\ell)\right) = \frac{p-1}{2}\left(S^2(1) + S^2(\ell)\right), \tag{8.4}$$

since $S^2(0) = 0$.

Now,

$$\begin{aligned}\sum_{m(\text{mod } p)} S^2(m) &= \sum_{m(\text{mod } p)} \sum_{\substack{s(\text{mod } p)\\ t(\text{mod } p)}} \left(\frac{s(s^2-m)}{p}\right)\left(\frac{t(t^2-m)}{p}\right) \\ &= \sum_{m,s,t} \left(\frac{st}{p}\right)\left(\frac{(m-s^2)(m-t^2)}{p}\right) \\ &= \sum_{s,t} \left(\frac{st}{p}\right) \sum_{m} \left(\frac{(m-s^2)(m-t^2)}{p}\right). \end{aligned} \tag{8.5}$$

By Lemma 8.2, (8.4) and (8.5), we deduce that

$$\begin{aligned}\frac{p-1}{2}\left(S^2(1) + S^2(\ell)\right) &= \sum_{\substack{s,t\\ s^2 \equiv t^2 (\text{mod } p)}} \left(\frac{st}{p}\right)(p-1) + \sum_{\substack{s,t\\ s^2 \not\equiv t^2 (\text{mod } p)}} \left(\frac{st}{p}\right)(-1) \\ &= \sum_{\substack{s,t\\ s^2 \equiv t^2 (\text{mod } p)}} \left(\frac{st}{p}\right)(p-1) - \left\{\sum_{s,t}\left(\frac{st}{p}\right) - \sum_{\substack{s,t\\ s^2 \equiv t^2 (\text{mod } p)}} \left(\frac{st}{p}\right)\right\} \\ &= p \sum_{\substack{s,t\\ s^2 \equiv t^2 (\text{mod } p)}} \left(\frac{st}{p}\right), \end{aligned}$$

where we have used Lemma 8.1 in the last equality. Next,

$$\sum_{\substack{s,t \\ s^2 \equiv t^2 (\mathrm{mod}\ p)}} \left(\frac{st}{p}\right) = \sum_{\substack{s,t \\ s \equiv t (\mathrm{mod}\ p)}} \left(\frac{st}{p}\right) + \sum_{\substack{s,t \\ s \equiv -t (\mathrm{mod}\ p)}} \left(\frac{st}{p}\right)$$
$$= \sum_{t (\mathrm{mod}\ p)} \left(\frac{t^2}{p}\right) + \sum_{t (\mathrm{mod}\ p)} \left(\frac{-t^2}{p}\right) = 2(p-1)$$

Hence we conclude that

$$\left(\frac{S(1)}{2}\right)^2 + \left(\frac{S(\ell)}{2}\right)^2 = p.$$

Now, if $2|S(m)$ then we would have found integers x and y such that

$$x^2 + y^2 = p.$$

To show that $2|S(m)$ for all integers m, we observe that

$$S(m) = \sum_{n=1}^{(p-1)/2} \left(\frac{n(n^2-m)}{p}\right) + \sum_{n=(p+1)/2}^{p-1} \left(\frac{n(n^2-m)}{p}\right)$$
$$= \sum_{n=1}^{(p-1)/2} \left(\frac{n(n^2-m)}{p}\right) + \sum_{n=1}^{(p-1)/2} \left(\frac{(p-n)((p-n)^2-m)}{p}\right)$$
$$= 2 \sum_{n=1}^{(p-1)/2} \left(\frac{n(n^2-m)}{p}\right),$$

where the last equality follows for the fact that $p \equiv 1 \pmod 4$. □

REMARK 8.4 Recently, H.H. Chan, L. Long and Y.F. Yang (see Amer. Math. Monthly, vol. 118, no. 4, (2011), pp. 316–326) showed the following observation: Let $p \equiv 1 \pmod 6$. Suppose a is any integer such that $x^3 \equiv a \pmod p$ is not solvable. Then

$$3p = x^2 + xy + y^2,$$

with

$$x = \sum_{\alpha=1}^{p} \left(\frac{\alpha^3+1}{p}\right) \quad \text{and} \quad y = \left(\frac{a}{p}\right) \sum_{\alpha=1}^{p} \left(\frac{\alpha^3+a}{p}\right).$$

9 Binary Quadratic forms

9.1 Fermat-Euler Theorem

A binary quadratic form is an expression of the form

$$f(x, y) = ax^2 + bxy + cy^2$$

where $a, b, c \in \mathbf{Z}$. We will assume that $ac \neq 0$. Representation of an integer by a binary quadratic form has attracted attention of many mathematicians in the past. For example, Fermat (see Theorem 1.31) observed that a prime can be represented as a sum of two squares if and only if $p \equiv 1 \pmod 4$.

From Theorem 1.31, we find that ODD primes of the form $x^2 + y^2$ can be determined by the Legendre condition

$$\left(\frac{-1}{p}\right) = 1,$$

since this condition is equivalent to the condition that $p \equiv 1 \pmod 4$.

It turns out that ODD primes of the form $x^2 + 2y^2$ and primes greater than 3 and primes of the form $x^2 + 3y^2$ are also determined completely by the conditions

$$\left(\frac{-2}{p}\right) = 1 \quad \text{and} \quad \left(\frac{-3}{p}\right) = 1,$$

respectively. A natural question to ask is therefore, can all primes greater than 5 and of the form $x^2 + ny^2$ be determined by a single condition

$$\left(\frac{-n}{p}\right) = 1?$$

The answer is no.

For example, one can show that

$$p = x^2 + 5y^2$$

if and only if

$$\left(\frac{-1}{p}\right) = 1 \quad \text{and} \quad \left(\frac{-5}{p}\right) = 1.$$

Here, we see that two conditions are needed to determine primes of the form

$x^2 + 5y^2$. In fact if we only have one condition

$$\left(\frac{-5}{p}\right) = 1,$$

then we are only able to conclude that

$$p = x^2 + 5y^2$$

or

$$p = 2x^2 + 2xy + 3y^2.$$

The binary quadratic forms $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$ both have *discriminant* $b^2 - 4ac = -20$. Furthermore these binary quadratic forms are "genuinely different". The additional condition for the Legendre symbol allows us to conclude that p is indeed of the form $x^2 + 5y^2$. In the following sections, we will explain the meaning of binary quadratic forms being "genuinely different."

9.2 Representations of integers by binary quadratic forms

DEFINITION 9.1 Given a binary quadratic form $ax^2+bxy+cy^2$ the discriminant (denoted usually by d or Δ) of the quadratic form is defined to be the number $b^2 - 4ac$.

REMARK 9.1 If we write

$$ax^2 + bxy + cy^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix},$$

then we observe that

$$\det \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} = ac - \frac{b^2}{4}.$$

In other words, we may define the discriminant of a binary quadratic form as

$$d = -4\det \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}.$$

THEOREM 9.2 Let d be an integer. There exists at least one binary quadratic form with integral coefficients and discriminant d, if and only if $d \equiv 0$ or $1 \pmod 4$.

Proof
Let $f(x,y) = ax^2+bxy+cy^2$ be a binary quadratic form of discriminant d. Since $b^2 \equiv 0$ or $1 \pmod 4$, $d = b^2 - 4ac \equiv 0$ or $1 \pmod 4$. Suppose $d \equiv 0 \pmod 4$. Then the form

$$x^2 - \frac{d}{4}y^2$$

has discriminant d. If $d \equiv 1 \pmod 4$, then

$$x^2 + xy - \left(\frac{d-1}{4}\right)y^2$$

has discriminant d. □

DEFINITION 9.2 A form $f(x,y)$ is called indefinite if it takes on both positive and negative values. The form is called positive semidefinite (or negative semidefinite) if $f(x,y) \geq 0$ (or $f(x,y) \leq 0$) for all integers x, y. A semidefinite form is called definite if in addition the only pair of integers x, y for which $f(x,y) = 0$ is $(x,y) = (0,0)$.

EXAMPLE 9.1 The form $f(x,y) = x^2 - 2y^2$ is indefinite. The form $f(x,y) = (x-y)^2$ is semidefinite and the form $f(x,y) = x^2 + y^2$ is positive definite form.

EXAMPLE 9.2 Let d be the discriminant of the form

$$f(x,y) = ax^2 + bxy + cy^2.$$

If $d < 0$ and $a > 0$, show that $f(x,y)$ is positive definite.

Solution

We see that

$$f(x,y) = a\left(\left(x + \frac{by}{2a}\right)^2 + \frac{4ac-b^2}{4a^2}y^2\right) = a\left(\left(x + \frac{by}{2a}\right)^2 - \frac{d}{4a^2}y^2\right).$$

This shows that $f(x,y) \geq 0$ since $d < 0$. If $f(x,y) = 0$, then we must have $y = 0$ and $x + by/(2a) = x = 0$. Therefore, $f(x,y)$ is positive definite.

From now on, we will assume $d < 0$ and $f(x,y)$ is positive definite. Since f is positive definite and $a = f(1,0) > 0$ and $c = f(0,1) > 0$, we deduce that $f(x,y) = ax^2 + bxy + cy^2$ with $a > 0$ and $c > 0$.

DEFINITION 9.3 We say that a quadratic form $f(x,y)$ represents an integer n if there exists integers k,ℓ such that

$$f(k,\ell)=n.$$

We say that the representation is proper if $(k,\ell)=1$; otherwise, it is improper.

REMARK 9.3 If p is an odd prime and $p\equiv 1 \pmod 4$, then p is a sum of two squares and the representation is proper.

THEOREM 9.4 Let $n>0$ and $d\neq 0$ be integers. There exists a binary quadratic form of discriminant d that represents n properly if and only if the congruence

$$x^2\equiv d \pmod{4n}$$

has a solution.

Proof

Suppose b is a solution of

$$x^2\equiv d \pmod{4n}.$$

Then $b^2=d+4nc$, for some integer c. The form

$$f(x,y)=nx^2+bxy+cy^2$$

has discriminant d and properly represents n since $f(1,0)=n$.

Next, suppose $f(k,\ell)=n$ and $(k,\ell)=1$. We claim that we can find a quadratic form $g(x,y)$ that takes the form

$$nx^2+Bxy+Cy^2.$$

Since $(k,\ell)=1$, there exist integers u,v such that $ku-\ell v=1$. Let $g(x,y)=f(kx+vy,\ell x+uy)$. In terms of matrices, we find that

$$g(x,y)=\begin{pmatrix}x & y\end{pmatrix}\begin{pmatrix}k & \ell\\ v & u\end{pmatrix}\begin{pmatrix}a & b/2\\ b/2 & c\end{pmatrix}\begin{pmatrix}k & v\\ \ell & u\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}.$$

Since

$$\det\begin{pmatrix}k & \ell\\ v & u\end{pmatrix}=ku-\ell v=1,$$

we deduce that the discriminant of $g(x,y)$, which is given by

$$-4\det\left(\begin{pmatrix}k & \ell\\ v & u\end{pmatrix}\begin{pmatrix}a & b/2\\ b/2 & c\end{pmatrix}\begin{pmatrix}k & v\\ \ell & u\end{pmatrix}\right)=-4\det\begin{pmatrix}a & b/2\\ b/2 & c\end{pmatrix}=b^2-4ac,$$

which is the discriminant of $f(x, y)$. Now,

$$\begin{aligned} g(x,y) = f(kx+vy, \ell x+uy) &= a(kx+vy)^2 + b(kx+vy)(\ell x+uy) + c(\ell x+uy)^2 \\ &= (ak^2+bk\ell+c\ell^2)x^2 + Bxy + Cy^2 \\ &= nx^2 + Bxy + Cy^2. \end{aligned}$$

The discriminant of $g(x, y)$ is

$$B^2 - 4nC = d.$$

This immediately implies that

$$x^2 \equiv d \pmod{4n}$$

has a solution. □

COROLLARY 9.5 Suppose $d \equiv 0$ or $1 \pmod 4$. If p is an odd prime, then there is a binary quadratic form of discriminant d that represents p if and only if

$$\left(\frac{d}{p}\right) = 1.$$

Proof

By Theorem 9.4, we conclude that

$$x^2 \equiv d \pmod{4p}$$

is solvable if p can be represented by a binary quadratic form of discriminant d. This implies that

$$x^2 \equiv d \pmod{p}$$

is solvable, or

$$\left(\frac{d}{p}\right) = 1.$$

Conversely, if $\left(\frac{d}{p}\right) = 1$ then there exists u such that

$$u^2 \equiv d \pmod{p}$$

is solvable. Note that $d \equiv 0$ or $1 \pmod 4$, observe that there exists v such that

$$v^2 \equiv d \equiv 0 \quad \text{or} \quad 1 \pmod 4.$$

By Chinese Remainder Theorem, we conclude that there exists $w \pmod{4p}$ with $w \equiv u \pmod p$ and $w \equiv v \pmod 4$. This integer w satisfies

$$x^2 \equiv d \pmod{4p}.$$

By Theorem 9.4, p is represented by a binary quadratic form of discriminant d. □

9.3 Equivalence of binary quadratic forms

We have seen in the proof of Theorem 9.4 that 2×2 matrices with entries in $\mathbf{Z}$ and determinant 1 play a role in the study of quadratic forms.

DEFINITION 9.4 Define

$$\mathrm{SL}_2(\mathbf{Z}) := \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} | \alpha, \beta, \gamma, \delta \in \mathbf{Z}, \alpha\delta - \beta\gamma = 1 \right\}.$$

DEFINITION 9.5 Denote $\mathcal{F}_d$ be the set of positive definite binary quadratic forms of discriminant $d < 0$.

DEFINITION 9.6 We say that two quadratic forms $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = Ax^2 + Bxy + Cy^2$ are related and write $f \sim g$ if there are integers $\alpha, \beta, \gamma, \delta \in \mathbf{Z}$ with $\alpha\delta - \beta\gamma = 1$, such that

$$g(x, y) = f(\alpha x + \gamma y, \beta x + \delta y).$$

REMARK 9.6 We may state the relation in terms of matrix in $\mathrm{SL}_2(\mathbf{Z})$. We say that $f \sim g$ if and only if there exists a matrix $M \in \mathrm{SL}_2(\mathbf{Z})$ such that

$$M \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} M^T = \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix},$$

if $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = Ax^2 + Bxy + Cy^2$.

THEOREM 9.7 The relation $\sim$ is an equivalence relation on $\mathcal{F}_d$.

Proof
Since $f(x, y) = f(x, y)$, $f \sim f$.
Suppose $f \sim g$, then we can write

$$g(x, y) = \begin{pmatrix} x & y \end{pmatrix} M \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} M^T \begin{pmatrix} x \\ y \end{pmatrix}$$

for some matrix $M \in \mathrm{SL}_2(\mathbf{Z})$. This implies that

$$f(x,y) = \begin{pmatrix} x & y \end{pmatrix} M^{-1} \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} (M^{-1})^T \begin{pmatrix} x \\ y \end{pmatrix}$$

and therefore, $g \sim f$.

Lastly, to check transitivity, we suppose that

$$h(x,y) = A'x^2 + B'xy + C'y^2.$$

Suppose $f \sim g$ and $g \sim h$. Then

$$\begin{aligned} g(x,y) &= \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\ &= \begin{pmatrix} x & y \end{pmatrix} M \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} M^T \begin{pmatrix} x \\ y \end{pmatrix} \end{aligned}$$

and

$$\begin{aligned} h(x,y) &= \begin{pmatrix} x & y \end{pmatrix} M' \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} (M')^T \begin{pmatrix} x \\ y \end{pmatrix} \\ &= \begin{pmatrix} x & y \end{pmatrix} M'M \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} (M'M)^T \begin{pmatrix} x \\ y \end{pmatrix}. \end{aligned}$$

Therefore, $f \sim h$. □

We have seen that $\sim$ is an equivalence relation on $\mathcal{F}_d$ and so, we can express $\mathcal{F}_d$ as a disjoint union of equivalence classes $[r] := \{f \in \mathcal{F}_d | f \sim r\}$. Let $C(d)$ be the set of equivalence classes. Is $C(d)$ finite? We will give an answer to this question in the next section.

9.4 Reduced forms

Let

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$$

and write

$$f(x,y) = ax^2 + bxy + cy^2$$

as

$$[a,b,c].$$

We define

$$M(f(x,y)) = M([a,b,c]) = f(\alpha x + \gamma y, \beta x + \delta y).$$

When

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

$$S([a,b,c]) = [c,-b,a].$$

When

$$T_m = \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix},$$

$$T_m([a,b,c]) = [a, b+2am, am^2+bm+c] = [a, b+2am, C].$$

We usually do not need the explicit form of C under T_m as it can be derived from $d = (b+2am)^2 - 4aC$.

DEFINITION 9.7 Let $f(x,y) = ax^2+bxy+cy^2 \in \mathcal{F}_d$. We say that $f(x,y)$ is reduced if

$$-a < b \leq a < c$$

or if

$$0 \leq b \leq a = c.$$

We will first show the following:

THEOREM 9.8 Each equivalence class of $\mathcal{F}_d$ under $\sim$ contains at least one reduced form.

Proof
Suppose

$$f = [a,b,c].$$

Let

$$\mathcal{F} := \{A \in \mathbf{Z}^+ | [A,B,C] \sim [a,b,c]\}.$$

Note that $\mathcal{F}$ is non-empty and because $f \sim f$ and $a > 0$ as f is positive definite. By the least integer axiom, there exists a smallest positive integer u in the set $\mathcal{F}$.

Let

$$g = [u,v,w]$$

such that $[u,v,w] \sim [a,b,c]$. Note that $u \leq w$. This is because if $w < u$, then

$$S([u,v,w]) = [w,-v,u]$$

will imply that $w \in \mathcal{F}$ and is smaller than u, which contradicts the minimality of u. This step implies that if $[u,v,w] \sim [a,b,c]$ then we can always conclude that $u \leq w$.

Next, by the Division Algorithm, we have

$$v = 2mu + r, -u < r \leq u.$$

Note that

$$T_{-m}([u, v, w]) = [u, v - 2mu, W] = [u, r, W].$$

We have already seen from the previous paragraph that $u \leq W$. If $u < W$, then $[u, r, W]$ is reduced. If $u = W$ and $r \geq 0$, then $[u, r, W]$ is reduced. We are left with $u = W$ and $r < 0$. In this case,

$$S([u, r, u]) = [u, -r, u],$$

and $[u, -r, u]$ is reduced. This completes the proof of the theorem. □

EXAMPLE 9.3 Find a reduced form g such that $g \sim [3, 2, 2]$.

Solution

We have $S([3, 2, 2]) = [2, -2, 3]$ and $T_1([2, -2, 3]) = [2, -2 + 4, 3] = [2, 2, 3]$. So we may take $g = [2, 2, 3]$.

Our next step is to show that if $f \in \mathcal{F}_d$, then f can be equivalent to exactly ONE reduced form. We will need a lemma before proving the above claim.

LEMMA 9.9 Let $f(x, y) = ax^2 + bxy + cy^2$ be a reduced positive definite form. If for some pair of integers α and β we have $(\alpha, \beta) = 1$ and $f(\alpha, \beta) \leq c$, then $f(\alpha, \beta) = a$ or c and the point (α, β) is one of the six points

$$\pm(1, 0), \pm(0, 1), \pm(1, -1).$$

Moreover, the number of proper representations of a by f is

$$\begin{cases} 2 & \text{if } a < c, \\ 4 & \text{if } 0 \leq b < a = c, \text{ and} \\ 6 & \text{if } a = b = c. \end{cases}$$

Proof

Suppose that $|\beta| \geq 2$. Then

$$\begin{aligned} 4af(\alpha, \beta) &= (2a\alpha + b\beta)^2 - d\beta^2 \geq -d\beta^2 \\ &\geq -4d = 16ac - 4b^2 > 8ac - 4b^2 \\ &\geq 4a^2 - 4b^2 + 4ac \geq 4ac. \end{aligned}$$

Thus, $f(\alpha, \beta) > c$ if $|\beta| \geq 2$. This implies that if $f(\alpha, \beta) \leq c$ then $|\beta| \leq 1$.

Now, suppose that $|\beta| = 1$ and $|\alpha| \geq 2$. Then

$$|2a\alpha + b\beta| \geq |2a\alpha| - |b\beta| \geq 4a - |b| \geq 3a.$$

Therefore,

$$\begin{aligned} 4af(\alpha, \beta) &= (2a\alpha + b\beta)^2 - d\beta^2 \geq 9a^2 - d\beta^2 \\ &= 9a^2 - d = 9a^2 + 4ac - b^2 > a^2 - b^2 + 4ac \geq 4ac. \end{aligned}$$

Thus, $f(\alpha, \pm 1) > c$.

Next, if $\beta = 0$ then since $(\alpha, \beta) = 1$, we conclude that $\alpha = \pm 1$.

Collecting what we obtain so far, we conclude that if $f(\alpha, \beta) \leq c$, then $|\beta| \leq 1$ and $|\alpha| \leq 1$. There are altogether eight points $(0, 0)$ is excluded since the greatest common divisor of 0 and 0 is not 1) (α, β) satisfying the above inequalities. These are

$$\pm(1, 0) \pm (0, 1), \pm(1, -1) \quad \text{and} \quad \pm (1, 1).$$

Next, since $b > -a$, we find that

$$f(\pm 1, \pm 1) = a + b + c > c.$$

Hence, $(1, 1)$ and $(-1, -1)$ are excluded as well.

We have thus arrived at the six possible solutions. The last assertion follows on observing that

$$f(\pm 1, 0) = a, f(0, \pm 1) = c \quad \text{and} \quad f(\pm 1, \mp 1) = a - b + c.$$

We observe that from the above computations, a and c are the smallest positive integer and second smallest positive integer represented by f respectively. □

THEOREM 9.10 Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = Ax^2 + Bxy + Cy^2$ be reduced positive definite quadratic forms. If $f \sim g$ then $f = g$.

Proof

The integer a is properly represented by $f = [a, b, c]$. Since $f \sim g$, a is represented by $[A, B, C]$. Since g is reduced, A is the smallest positive integer properly represented by g and this implies that $A \leq a$. By interchanging the roles of f, a and g, A respectively, we deduce that $a \leq A$ and thus, $A = a$.

Suppose that there are more than 2 representations of a by f. Then by Lemma 9.9, we know that $c = a$. Since $f \sim g$, there are also more than 2 representations of $a = A$ by g. This implies that $C = A$. We now have $f = [a, b, a]$ and $g = [a, B, a]$. But $b^2 - 4ac = B^2 - 4ac$ implies that $b^2 = B^2$, or $b = \pm B$. Since f and g are both reduced and $a = c$, we conclude that both b, B are non-negative and $b = B$. Therefore, $f = g$.

Suppose that there are exactly two representations of a by f. Then $c > a$.

Similarly, $C > a$. Now, c is represented by f and therefore it is represented by g. But C is the second smallest positive integer properly represented by g, and $c > a$, this implies that $C \leq c$ since c is the second smallest positive integer properly represented by f. Once again, by interchanging the roles of f, c and g, C respectively, we conclude that $c \leq C$ and thus $c = C$. We now have $f = [a, b, c]$ and $g = [a, B, c]$.

Now, since $c > a$ there are only two representation of a in terms of $g(x, y)$, namely $(\pm 1, 0)$. Since $g(x, y) = f(\alpha x+\gamma y, \beta x+\delta y)$ this implies that $f(\pm\alpha, \pm\beta) = a$. But the solutions of $f(x, y) = a$ are $(\pm 1, 0)$ and so $\alpha = \pm 1$. Similarly the solutions to $g(x, y) = c$ are $(0, \pm 1)$ and this translates that $f(\pm\gamma, \pm\delta) = c$. Since the only solutions of $f(x, y) = c$ are $(0, \pm 1)$, we deduce that $\gamma = 0$ and $\delta = \pm 1$. Now $\alpha\delta - \beta\gamma = 1$ implies that α and δ have the same sign. Therefore $g(x, y) = f(\pm x, \pm y) = f(x, y)$ and this completes the proof.

□

THEOREM 9.11 Let f be a reduced positive definite binary quadratic form whose discriminant d is not a perfect square. Then $0 < a \leq \sqrt{-d/3}$. The number of reduced forms of a given nonsquare discriminant d is finite.

Proof

We see that

$$-d = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2.$$

Hence,

$$a \leq \sqrt{-d/3}.$$

Now for each $a \leq \sqrt{-d/3}$, we determined b and c for which $[a, b, c]$ is reduced by using the inequality $-a < b \leq a$ and the equation

$$b^2 - 4ac = d.$$

This implies that there are finitely many reduced forms. □

EXAMPLE 9.4 If $d = -4$, then $a = 1$. From $b^2 - 4ac = -4$, we conclude that b is even and hence $b = 0$. This implies that the only reduced form with discriminant -4 is $x^2 + y^2$. In Theorem 9.4, we find that if $\left(\frac{-1}{p}\right) = 1$, then p is represented by a binary quadratic form with discriminant -4. Since there is only one reduced form with discriminant -4 and all binary quadratic forms must be equivalent to $x^2 + y^2$, we conclude that p must a sum of two squares. This gives another proof of the classification of primes which are sum of two squares.

EXAMPLE 9.5 Consider $d = -20$. Then $a \leq 2$. From $b^2 - 4ac = -20$, we conclude that b has to be even. If $a = 1$, then $b = 0$ and the only reduced form with $a = 1$ is x^2+5y^2. When $a = 2$, $b = 0$ or 2. There is no reduced corresponding to $b = 0$ since there are no integer c satisfying $-8c = -20$. Therefore $b = 2$ and we conclude that $c = 3$. The reduced form with $a = 2$ is $2x^2 + 2xy + 3y^2$.

REMARK 9.12 There is a formula to compute the number of reduced binary quadratic form of discriminant $d < 0$. For example if $d \equiv 1 \pmod 4$ and $|d| > 3$, then the number is

$$\frac{-1}{|d|} \sum_{\substack{(n,d)=1 \\ 1<n<|d|}} n \left(\frac{n}{|d|}\right).$$

For example, if $|d| = 11$, we have

$$\frac{1}{11}\{1 + 4 + 9 + 5 + 3 - 2 - 6 - 7 - 8 - 10\} = 1.$$

10 Form Class groups

10.1 The set $C(d)$

Let $d < 0, d \equiv 0, 1 \pmod 4$ and $\mathcal{F}_d$ be the set of binary quadratic forms with discriminant d. We have seen in the last Chapter that $\mathcal{F}_d$ is a disjoint unions of equivalence classes obtained from the equivalence relation $\sim$. We have show that the set of equivalence classes $C(d) = \{[f]\}$ is finite and each equivalence class represented by a reduced form. In this chapter, following the work of Gauss and Dirichlet, we construct a binary operation $\bullet$ on $C(d)$ and show that $(C(d), \bullet)$ is a finite abelian group.

In this chapter, we will assume that $d < 0, d \equiv 1 \pmod 4$ (respectively $0 \pmod 4$) and $|d|$ (respectively $|d|/4$) is square-free (i.e. it is not divisible by any integer $k^2, k > 1$). This additional assumption is to guarantee that the positive definite binary quadratic form

$$f(x, y) = ax^2 + bxy + cy^2$$

with discriminant d has the additional property that the gcd $(a, b, c) = 1$. A quadratic form with such a property is called a primitive form.

Let $C(d)$ be the set of equivalence classes of positive definite binary quadratic forms. We have seen that each class contains a unique reduced form and hence, $|C(d)|$ is finite. We wish to obtain a binary operation $\bullet$ on $C(d)$ and obtain a group structure on $C(d)$. Let $\mathcal{C}_1, \mathcal{C}_2 \in C(d)$.

DEFINITION 10.1 Two binary quadratic forms $[a, b, c]$ and $[a', b', c']$ of discriminant d are *concordant* if the following three conditions are met:

(a) $aa' \neq 0$,
(b) $b = b'$,
(c) $a|c'$ and $a'|c$.

REMARK 10.1 Note that if $[a, b, c]$ and $[a', b', c']$ are concordant, then

$$b^2 - 4ac = b'^2 - 4a'c' = b^2 - 4a'c'.$$

This gives $4ac = 4a'c'$. Now $a|c'$ implies that $c' = aC$. This gives $c = a'C$. Therefore, we conclude that $[a, b, c] = [a, b, a'C]$ and $[a', b', c'] = [a', b, aC]$.

We will show later that given $\mathcal{C}_1$ and $\mathcal{C}_2$, there are representatives of $\mathcal{C}_1$ and $\mathcal{C}_2$ of the form $[a, B, Ca']$ and $[a', B, Ca]$ respectively. Note that $[a, B, Ca']$ and $[a', B, Ca]$ are concordant. We then define

$$[a, B, Ca'] \circ [a', B, Ca] := [aa', B, C]$$

and that [1]

$$\mathcal{C}_1 \bullet \mathcal{C}_2 := [[aa', B, C]].$$

Our operation $\circ$ is motivated by the following identity of Gauss [2]:

$$(a_1x_1^2 + bx_1y_1 + a_2cy_1^2)(a_2x_2^2 + bx_2y_2 + a_1cy_2^2) = a_1a_2x^2 + bxy + cy^2$$

where

$$x = x_1x_2 - cy_1y_2, y = a_1x_1y_2 + a_2x_2y_1 + by_1y_2.$$

This identity of Gauss-Dirichlet can be proved by observing that

$$f(x, y) = ax^2 + bxy + cy^2 = \frac{1}{4a}N\left(2ax + by + \sqrt{d}y\right)$$

with $d = b^2 - 4ac$ and $N(u + v\sqrt{d}) = u^2 - dv^2$.

The main difficulty in showing that $(C(d), \bullet)$ is a group is to show that $\bullet$ is well-defined. But first, we will show that given $\mathcal{C}_1$ and $\mathcal{C}_2$, we can always find pairs of forms in $\mathcal{C}_1$ and $\mathcal{C}_2$ of the form $[a, B, Ca']$ and $[a', B, Ca]$ for some integers B and C. To do this, we need the following theorem:

THEOREM 10.2 Suppose f is a primitive positive definite binary quadratic form and k is a nonzero integer, then there exists an integer n properly represented by f with the property that $(n, k) = 1$.

Proof
Let $k = \prod_{j=1}^{m} p_j^{\alpha_j}$. Note that for each prime $p_j|k$, one of the numbers $f(1, 0)$, $f(1, 1)$ and $f(0, 1)$ is relatively prime to p_j. For if this were not the case, then there will be a number ℓ that divides $f(1, 0) = a$, $f(1, 1) = a + b + c$ and $f(0, 1) = c$. This number ℓ would divide b as well, which implies that f is not primitive.

Let $(x_j, y_j) \in \{(1, 0), (0, 1), (1, 1)\}$ be such that $f(x_j, y_j)$ is relative prime to p_j for $1 \leq j \leq m$. Now, by Chinese Remainder Theorem, there are integers u, v satisfying the congruences

$$x \equiv x_j \pmod{p_j^{\alpha_j}} \quad \text{and} \quad y \equiv y_j \pmod{p_j^{\alpha_j}}, 1 \leq j \leq m.$$

[1] The choice of representatives $[a, B, Ca']$ and $[a', B, Ca]$ is so that C can be computed as $C = (B^2 - d)/(4aa')$.
[2] This approach is due to Dirichlet.

Note that $N = f(u, v)$ is the number relatively prime to k. There is no guarantee that the integer N we found is properly represented by f. If N is properly represented by f, then we choose $n = N$. Suppose N is not properly represented by f. Let $(u, v) = d > 1$. Then $u = ds$ and $v = dt$ implies that

$$d^2(as^2 + bst + ct^2) = N,$$

or

$$N/d^2 = as^2 + bst + ct^2.$$

Since $(s, t) = (u/d, v/d) = 1$, we see that $n = N/d^2$ is properly represented by f and $(n, k) = 1$ since $(N, k) = 1$. □

EXAMPLE 10.1 Let $f(x, y) = 2x^2 + 3y^2$ and $k = 12$. Now, $f(0, 1) = 3$ and is relatively prime to 4 and $f(1, 0) = 2$ and is relatively prime to 3. We find that $u = 4$ satisfies $u \equiv 0 \pmod 4$ and $u \equiv 1 \pmod 3$, $v = 9$ satisfies $v \equiv 1 \pmod 4$ and $v \equiv 0 \pmod 3$. Note that $f(4, 9) = 275$ is relatively prime to 12.

Let $\mathcal{C}_1 = [f]$ and $\mathcal{C}_2 = [g]$. Suppose $f = [a, b, c]$. By Theorem 10.2, there exists a' represented by g such that $(2a, a') = 1$. We replace g by $[a', b', c']$. Using Chinese Remainder Theorem, there exists a unique B modulo $2aa'$ such that

$$B \equiv b \pmod{2a} \quad \text{and} \quad B \equiv b' \pmod{a'}.$$

Let

$$B = b + 2aK \quad \text{and} \quad B = b' + a'M. \tag{10.1}$$

Then $B^2 - d = 4ac + 4a^2K^2 + 4baK = 4a'c' + (a')^2M^2 + 2b'a'M$. This implies that $(a')^2M^2 + 2b'a'M \equiv 0 \pmod 4$. Since a' is odd, we conclude that M is even. Let $M = 2L$. Note that

$$[a, b, c] \sim [a, b + 2aK, C^*]$$

and

$$[a', b', c'] \sim [a', b' + 2La', C^\dagger].$$

Now,

$$B^2 - 4aC^* = B^2 - 4a'C^\dagger$$

implies that

$$aC^* = a'C^\dagger.$$

Since $(a, a') = 1$, we conclude that

$$C^* = Ca'$$

for some integer C and this yields

$$C^\dagger = Ca.$$

In other words,

$$[a,b,c] \sim [a,B,Ca'] \quad \text{and} \quad [a',b',c'] \sim [a',B,Ca].$$

We have thus shown that $\mathcal{C}_1$ and $\mathcal{C}_2$ contains forms of the form $[a,B,Ca']$ and $[a',B,Ca]$ (which are concordant) respectively and $\bullet$ is defined as

$$\mathcal{C}_1 \bullet \mathcal{C}_2 = [[aa',B,C]].$$

The above observation that b and b' having the same parity allows us to replace (10.1) by

$$B = b + 2aK \quad \text{and} \quad B = b' + 2a'L \tag{10.2}$$

whenever a' is odd.

10.2 $C(d)$ is a finite abelian group

We will show later that $\bullet$ is well defined. But first, assuming that $\bullet$ is well defined, we want to show that $(C(d), \bullet)$ is a finite abelian group.

To simplify our treatment, we assume $d \equiv 0 \pmod 4$. The case for $d \equiv 1 \pmod 4$ is similar. Let $\mathcal{C}_0 = [[1,0,-d/4]]$. We will show that $\mathcal{C}_0$ is an identity for $(C(d), \bullet)$. Take $\mathcal{C}_1 = [[a,b,c]]$. Now,

$$[1,0,-d/4] \sim [1,b,c']$$

since b is even. Therefore,

$$\mathcal{C}_0 \bullet \mathcal{C}_1 = [[1,0,-d/4]] \bullet [[a,b,c]] = [[1,b,ac] \circ [a,b,c]] = [[a,b,c]] = \mathcal{C}_1.$$

Hence, $\mathcal{C}_0$ is the identity.

Next, let $\mathcal{C}_1 = [[a,b,c]]$. We claim that $\mathcal{C}_2 = [[a,-b,c]]$ is the inverse of $\mathcal{C}_1$.

$$[a,-b,c] \sim [c,b,a].$$

Now both $[a,b,c]$ and $[c,b,a]$ are of the forms $[u,v,wu']$ and $[u',v,wu]$ with $w = 1$ and hence the composition of the quadratic forms exists and is given by

$$[a,b,c] \circ [c,b,a] = [ac,b,1].$$

Now,

$$[ac,b,1] \sim [1,-b,ac] \sim [1,0,-d/4].$$

Hence,

$$\mathcal{C}_1 \bullet \mathcal{C}_2 = \mathcal{C}_0.$$

To show associativity, we let $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ be three elements in $C(d)$. Using Theorem 10.2, we can find a, a', a'' such that $a, a', a'', 2$ are pairwise relatively prime. We construct B such that

$$B \equiv b \pmod{2a}, B \equiv b' \pmod{a'} \quad \text{and} \quad B \equiv b'' \pmod{a''}.$$

Note that

$$[[a, B, c_1]] \bullet [[a', B, c_2]] = [[aa', B, C]]$$

and

$$[[aa', B, C]] \bullet [[a'', B, c_3]] = [[aa'a'', B, C_1]].$$

Similarly,

$$\mathcal{C}_1 \bullet (\mathcal{C}_2 \bullet \mathcal{C}_3) = [[aa'a'', B, C_2]].$$

Note that $C_1 = C_2$ and we are done.

EXAMPLE 10.2 Show that $(C(-56), \bullet)$ is a cyclic group of order 4.

Solution

The elements in $C(-56)$ are

$$[[1, 0, 14]], [[2, 0, 7]], [[3, 2, 5]], [[3, -2, 5]].$$

Since

$$[[3, 2, 5]]^{-1} = [[3, -2, 5]] \neq [[3, 2, 5]],$$

we conclude that the group is cyclic of order 4. For, if G is a Klein 4-group, the inverse of $x \in G$ must satisfy $x^{-1} = x$.

Alternatively, we may compute $[[3, 2, 5]]\bullet[[3, 2, 5]]$. Note that $[3, 2, 5] \sim [5, -2, 3]$ and we determine a B such that $B \equiv 2 \pmod 6$ and $B \equiv -2 \pmod 5$. This choose $B = 8$. This yields $[3, 2, 5] \sim [3, 8, C]$ and $[5, -2, 3] \sim [5, 8, C']$ and

$$[[3, 2, 5]] \bullet [[3, 2, 5]] = [[15, 8, 2]] = [[2, -8, 15]] = [[2, 0, 7]]$$

and so $C(-56)$ is cyclic of order 4 since every element in a Klein 4 group has order 2.

10.3 The operation • is well defined

The most difficult part in showing $(C(d), \bullet)$ is a group is to show that $\bullet$ is well defined. In other words, if we have

$$[u, V, Wu'] \sim [a, B, Ca']$$

and

$$[u', V, Wu] \sim [a', B, Ca],$$

we want to show that

$$[uu', V, W] \sim [aa', B, C].$$

We will complete this task in a few steps. Let

$$f_1 = [a, B, Ca'], f_2 = [u, V, Wu']$$

and

$$g_1 = [a', B, Ca], g_2 = [u', V, Wu]$$

be such that

$$f_1 \sim f_2 \quad \text{and} \quad g_1 \sim g_2.$$

Step 1

Suppose $f_1 = f_2$ and $(a, u') = 1$. Since $f_1 = f_2$, we have $a = u$ and $B = V$. Our aim is to show that if

$$g_1 \sim g_2,$$

then

$$f_1 \circ g_1 \sim f_1 \circ g_2.$$

This is equivalent to showing that

$$[aa', B, C] \sim [au', B, W].$$

Now, since $g_1 \sim g_2$, there is a matrix

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$$

such that (note that we have $u = a$ and so $Wu = Wa$)

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} a' & B/2 \\ B/2 & Ca \end{pmatrix} = \begin{pmatrix} u' & B/2 \\ B/2 & Wa \end{pmatrix} \begin{pmatrix} \delta & -\gamma \\ -\beta & \alpha \end{pmatrix}. \tag{10.3}$$

From the $(1, 2)$-entry of the matrices on both sides of (10.3), we find that

$$\alpha B/2 + Ca\beta = -u'\gamma + \alpha B/2.$$

This shows that

$$\beta Ca = -u'\gamma.$$

By assumption, $(a, u') = 1$ and hence,

$$\gamma/a \in \mathbf{Z}.$$

Next, from the $(1, 1)$-entry, $(2, 1)$-entry and $(2, 2)$-entry of both sides of (10.3), we find that

$$\alpha a' + \frac{\beta B}{2} = \delta u' - \frac{\beta B}{2},$$
$$\gamma a' + \frac{\delta B}{2} = \frac{\delta B}{2} - \beta W a$$

and

$$\frac{\gamma B}{2} + \delta C a = -\frac{\gamma B}{2} + W a \alpha.$$

This implies that

$$\begin{pmatrix} \alpha & \beta a \\ \gamma/a & \delta \end{pmatrix} \begin{pmatrix} aa' & B/2 \\ B/2 & C \end{pmatrix} = \begin{pmatrix} au' & B/2 \\ B/2 & W \end{pmatrix} \begin{pmatrix} \delta & -\gamma/a \\ -\beta a & \alpha \end{pmatrix}.$$

Hence,

$$[aa', B, C] \sim [au', B, W].$$

Step 2

Suppose $(a, u') = 1$ and $B = V$. We have seen from Step 1 that $f_1 \circ g_1 \sim f_1 \circ g_2$. Applying Step 1 again with (f_1, g_2) replaced by (g_2, f_1), and noting that $(u', a) = 1$, we deduce that $g_2 \circ f_2 \sim g_2 \circ f_1$. Hence,

$$f_1 \circ g_1 \sim f_1 \circ g_2 = g_2 \circ f_1 \sim g_2 \circ f_2 = f_2 \circ g_2.$$

Step 3

Assume that $(aa', uu') = 1$. Note that in this step, we are dropping the assumption that $B = V$. Without loss of generality, assume that uu' is odd. By Chinese Remainder Theorem, there is a solution to

$$x \equiv B \pmod{2aa'} \quad \text{and} \quad x \equiv V \pmod{uu'}.$$

Let this solution be B^* and we observe that

$$B^* = B + 2aa'n_1 = V + uu'm.$$

By (10.2), we conclude that m is even and write $m = 2n_2$. In other words, we have

$$B^* = B + 2aa'n_1 = V + 2uu'n_2.$$

Let

$$F_1 = \begin{pmatrix} 1 & 0 \\ a'n_1 & 1 \end{pmatrix} ([a, B, Ca']) = [a, B^*, C_1]$$

and

$$G_1 = \begin{pmatrix} 1 & 0 \\ an_1 & 1 \end{pmatrix} ([a', B, Ca]) = [a', B^*, C_1'].$$

Note that

$$f_1 \sim F_1 \quad \text{and} \quad g_1 \sim G_1$$

and

$$f_1 \circ g_1 = [aa', B, C]$$

and

$$F_1 \circ G_1 = [aa', B^*, C_1^*].$$

Now,

$$\begin{aligned}\begin{pmatrix} 1 & 0 \\ n_1 & 1 \end{pmatrix} (f_1 \circ g_1) &= \begin{pmatrix} 1 & 0 \\ n_1 & 1 \end{pmatrix} ([aa', B, C]) \\ &= [aa', B^*, C_1^*]\end{aligned}$$

implies that

$$f_1 \circ g_1 \sim F_1 \circ G_1.$$

Using similar argument with f_1, g_1, n_1 replaced by f_2, g_2, n_2, we deduce that

$$f_2 \circ g_2 = F_2 \circ G_2$$

where

$$F_2 = \begin{pmatrix} 1 & 0 \\ u'n_2 & 1 \end{pmatrix} ([u, V, Wu']) = [u, B^*, C_2]$$

and

$$G_2 = \begin{pmatrix} 1 & 0 \\ un_2 & 1 \end{pmatrix} ([u', V, Wu]) = [u', B^*, C_2'].$$

Since the coefficient of the xy-term in F_1, F_2, G_1, G_2 is B^* and $(a, u') = 1$, by Step 2, we deduce that

$$F_1 \circ G_1 \sim F_2 \circ G_2.$$

But

$$f_1 \circ g_1 \sim F_1 \circ G_1$$

and

$$f_2 \circ g_2 \sim F_2 \circ G_2.$$

Combining the three relations, we conclude that

$$f_1 \circ g_1 \sim f_2 \circ g_2.$$

Step 4

We now drop the condition $(aa', uu') = 1$. Recall again that $f_1 = [a, B, Ca']$, $f_2 = [u, V, Wu']$ and $g_1 = [a', B, Ca]$, $g_2 = [u', V, Wu]$. Choose s such that $(s, aa'uu') = 1$ where s is an integer which can be represented by f_1. Moreover, we can find a form f such that $f \sim f_1$ and $f \sim f_2$ with the property that

$$f = [s, B', C'].$$

Choose s' such that $(s', 2aa'uu's) = 1$ where s' is an integer which can be

represented by g_1. The insertion of 2 in the gcd condition is to guarantee that s' is odd. Note that there is a form g such that $g \sim g_1$ and $g \sim g_2$ with

$$g = [s', B'', C''].$$

We remark here that the conditions on the gcd's are to guarantee that $(s, s') = 1$, $(ss', aa') = (ss', uu') = 1$. Since $(s, s') = 1$, we can find F, G with $F \sim f$ and $G \sim g$ and

$$F = [s, B^*, C_1^*] \quad \text{and} \quad G = [s', B^*, C_2^*],$$

with

$$B^* \equiv B' \pmod{2s} \quad \text{and} \quad B^* \equiv B'' \pmod{s'}.$$

Since $(ss', aa') = 1$, by Step 3, we conclude that

$$F \circ G \sim f_1 \circ g_1.$$

Similarly, since $(ss', uu') = 1$, by Step 3, we find that

$$F \circ G \sim f_2 \circ g_2.$$

Hence, we conclude that

$$f_1 \circ g_1 \sim F \circ G \sim f_2 \circ g_2.$$

This shows that $\bullet$ is a well defined operation and this completes the proof that $(C(d), \bullet)$ is a finite abelian group.

11 Continued fractions and Pell's equations

11.1 Pell's equations

DEFINITION 11.1 Let d be a positive integer which is not a perfect square. A diophantine equation $x^2 - dy^2 = 1$ is known as Pell's equation.

In this Chapter, we will show that for non-square positive integer d, Pell's equation is always solvable. The norm of $a + b\sqrt{d}$ is defined by $N(a + b\sqrt{d}) = 1$. It satisfies $N(\alpha\beta) = N(\alpha)N(\beta)$ if $\alpha = a + b\sqrt{d}$ and $\beta = a' + b'\sqrt{d}$. It turns out that if $N(a + b\sqrt{d}) = 1$ then $N((a + b\sqrt{d})^n) = (N(a + b\sqrt{d}))^n = 1$. Therefore, if $(a + b\sqrt{d})^n = u_n + v_n\sqrt{d}$, then $u_n^2 - dv_n^2 = 1$. So if $x^2 - dy^2 = 1$ has a solution, it has infinitely many solutions.

11.2 Continued fractions

Given a rational fraction u_0/u_1 such that $(u_0, u_1) = 1$ and $u_1 > 0$, we may write using the Euclidean algorithm,

$$\begin{aligned}
u_0 &= u_1 a_0 + u_2, 0 < u_2 < u_1, \\
u_1 &= u_2 a_1 + u_3, 0 < u_3 < u_2, \\
&\vdots \qquad\qquad \vdots \\
u_{j-1} &= u_j a_{j-1} + u_{j+1}, 0 < u_{j+1} < u_j, \\
u_j &= u_{j+1} a_j.
\end{aligned}$$

Let

$$\xi_i = \frac{u_i}{u_{i+1}}.$$

By using the above equations, we find that

$$\xi_0 = a_0 + \frac{1}{\xi_1} = \cdots = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{j-1} + \cfrac{1}{a_j}}}}.$$

This is a continued fraction expansion of ξ_0 or u_0/u_1. We use the notation

$$< a_0, a_1, \cdots, a_j >$$

to represent the above continued fraction. Note that

$$\begin{aligned} < x_0, x_1, \cdots, x_j > &= x_0 + \frac{1}{< x_1, \cdots, x_j >} \\ &= \left\langle x_0, x_1, \cdots, x_{j-2}, x_{j-1} + \frac{1}{x_j} \right\rangle. \end{aligned}$$

11.3 Infinite continued fraction

Let $a_0, a_1, a_2, \cdots$ be an infinite sequence of integers, all positive except perhaps a_0. We define two sequences of integers $\{h_n\}$ and $\{k_n\}$ inductively as follows :

$$\begin{aligned} h_{-2} = 0, h_{-1} = 1, h_i = a_i h_{i-1} + h_{i-2} \quad \text{for } i \geq 0 \\ k_{-2} = 1, k_{-1} = 0, k_i = a_i k_{i-1} + k_{i-2} \quad \text{for } i \geq 0. \end{aligned}$$

THEOREM 11.1 Let x be a positive real number. For positive integer $n \geq 1$,

$$< a_0, a_1, \cdots, a_{n-1}, x >= \frac{x h_{n-1} + h_{n-2}}{x k_{n-1} + k_{n-2}}.$$

Proof
When $n = 1$, we find that

$$< a_0, x >= a_0 + \frac{1}{x} = \frac{a_0 x + 1}{x} = \frac{x h_0 + h_{-1}}{x k_0 + k_{-1}}.$$

We now prove the theorem by induction. The induction step follows from the following computations:

$$\begin{aligned} < a_0, a_1, \cdots, a_n, x > &= \left\langle a_0, a_1, \cdots, a_{n-1}, a_n + \frac{1}{x} \right\rangle \\ &= \frac{(a_n + 1/x)h_{n-1} + h_{n-2}}{(a_n + 1/x)k_{n-1} + k_{n-2}} \\ &= \frac{x(a_n h_{n-1} + h_{n-2}) + h_{n-1}}{x(a_n k_{n-1} + k_{n-2}) + k_{n-1}} \\ &= \frac{xh_n + h_{n-1}}{xk_n + k_{n-1}}. \end{aligned}$$

□

If we let $x = a_n$ in Theorem 11.1, then we immediately obtain the following:

THEOREM 11.2 Let $n \geq 1$ be an integer. If $r_n =< a_0, a_1, \cdots, a_n >$, then

$$r_n = \frac{h_n}{k_n}.$$

DEFINITION 11.2 The expression

$$r_i =< a_0, a_1, \cdots, a_i >= \frac{h_i}{k_i}$$

is called the i-th convergent of the continued fraction $< a_0, a_1, \cdots, a_n >$.

THEOREM 11.3 For $i \geq 2$,

$$h_i k_{i-1} - h_{i-1} k_i = (-1)^{i-1} \tag{11.1}$$

$$r_i - r_{i-1} = \frac{(-1)^{i-1}}{k_i k_{i-1}} \tag{11.2}$$

$$h_i k_{i-2} - h_{i-2} k_i = (-1)^i a_i \tag{11.3}$$

and

$$r_i - r_{i-2} = \frac{(-1)^i a_i}{k_i k_{i-2}}. \tag{11.4}$$

Proof

Note that $h_{-1}k_{-2} - h_{-2}k_{-1} = 1$. Continuing the proof by induction, we suppose that

$$h_{i-1}k_{i-2} - h_{i-2}k_{i-1} = (-1)^{i-2}.$$

Then

$$\begin{aligned} h_i k_{i-1} - h_{i-1} k_i &= (a_i h_{i-1} + h_{i-2}) k_{i-1} - h_{i-1}(a_i k_{i-1} + k_{i-2}) \\ &= -(h_{i-1} k_{i-2} - h_{i-2} k_{i-1}) = (-1)^{i-1}, \end{aligned}$$

and this completes the proof of (11.1).

Identity (11.2) follows by dividing (11.1) by $k_i k_{i-1}$.

Identity (11.3) can be derived directly as follow:

$$\begin{aligned} h_i k_{i-2} - h_{i-2} k_i &= (a_i h_{i-1} + h_{i-2}) k_{i-2} - h_{i-2}(a_i k_{i-1} + k_{i-2}) \\ &= a_i (h_{i-1} k_{i-2} - h_{i-2} k_{i-1}) = (-1)^i a_i. \end{aligned}$$

Dividing the above identity by $k_i k_{i-2}$ we obtain (11.4). □

From (11.4), we find that

$$r_{2j-1} > r_{2j+1}$$

and

$$r_{2j+2} > r_{2j}.$$

From (11.2), we find that for a fixed positive j, the following inequalities hold:

$$r_2 < r_4 < \cdots < r_{2j} < r_{2j-1} < r_{2j-3} < \cdots < r_3.$$

This shows that the sequence $\{r_{2j}\}_{j=1}^{\infty}$ is bounded above by r_3 and the sequence $\{r_{2j-1}\}_{j=1}^{\infty}$ is bounded below by r_2. These facts led us to the following theorem:

THEOREM 11.4 The sequence $\{r_{2j}\}$ is monotonic increasing, bounded above by r_1, and the sequence $\{r_{2j-1}\}$ is monotonic decreasing and bounded below by r_0. The limit $\lim_{j\to\infty} r_j$ exists.

The existence of the limits of $\{r_{2j}\}$ and $\{r_{2j-1}\}$ follows from the Monotone sequence theorem. From (11.2), we find that

$$\lim_{j\to\infty} (r_{2j} - r_{2j-1}) = \lim_{j\to\infty} \frac{(-1)^{j-1}}{k_j k_{j-1}} = 0.$$

DEFINITION 11.3 An infinite sequence $a_0, a_1, \cdots$ of integers, all positive except perhaps for a_0, determines an infinite simple continued fraction $< a_0, a_1, a_2, \cdots >$. The value of $< a_0, a_1, a_2, \cdots >$ is defined to be

$$\lim_{n\to\infty} < a_0, a_1, a_2, \cdots, a_n > .$$

Note that this limit is the same as $\lim_{j\to\infty} r_j$.

11.4 A simple Lemma and primes of the form $x^2 + y^2$

We now establish a simple inequality and apply it to the study of primes of the form $x^2 + y^2$.

LEMMA 11.5 Let

$$\xi =< a_0, a_1, \cdots, a_n, \cdots > .$$

Then

$$|\xi - r_n| < |r_n - r_{n+1}| .$$

Proof
If $n = 2j$, then by (11.2),

$$r_{2j+1} - r_{2j} > 0.$$

Now $\{r_{2j}\}_{j=1}^{\infty}$ is increasing, and $\{r_{2j+1}\}_{j=1}^{\infty}$ is decreasing, we conclude that

$$0 < \xi - r_{2j} < r_{2j+1} - r_{2j}$$

and

$$\xi - r_{2j} > 0 > r_{2j} - r_{2j+1}.$$

Hence,

$$|\xi - r_{2j}| < |r_{2j} - r_{2j+1}| .$$

The argument is similar for odd integer $2k + 1$. This completes the proof of the Lemma. □

Now, let $p \equiv 1 \pmod 4$ be an odd prime. Then there exists a positive u such that

$$u^2 \equiv -1 \pmod p.$$

Let

$$\frac{u}{p} =< a_0, a_1, \cdots, a_\ell > .$$

Let j be such that

$$k_j < \sqrt{p} < k_{j+1}. \tag{11.5}$$

By Lemma 11.5, we conclude that

$$\left|\frac{u}{p} - r_j\right| < |r_{j+1} - r_j| < \frac{1}{k_j k_{j+1}} < \frac{1}{k_j\sqrt{p}},$$

where the second last inequality follows from (11.2). This implies that

$$|uk_j - h_j p| < \sqrt{p}. \tag{11.6}$$

Now, let $x = k_j$ and $y = uk_j - h_j p$. By (11.5) and (11.6), we find that

$$0 < x^2 + y^2 < |k_j|^2 + |uk_j - h_j p|^2 < 2p.$$

Furthermore,

$$x^2 + y^2 \equiv k_j^2 + u^2 k_j^2 \equiv 0 \pmod{p}$$

since

$$u^2 \equiv -1 \pmod{p}.$$

Hence,

$$p = x^2 + y^2.$$

This gives another proof of the fact that if $p \equiv 1 \pmod 4$ is an odd prime, it is a sum of two squares. This proof is due to C. Hermite.

11.5 Solutions to Pell's equations

Let ξ be an irrational number and let $< a_0, a_1, \cdots >$ be the continued fraction representation of ξ. We have

THEOREM 11.6 Let a/b be a rational number with positive denominator.

(I) If

$$|\xi b - a| < |\xi k_n - h_n|$$

for some $n \geq 0$, then $b \geq k_{n+1}$.

(II) If

$$\left|\xi - \frac{a}{b}\right| < \left|\xi - \frac{h_n}{k_n}\right|$$

for some $n \geq 1$, then $b > k_n$.

Note that (II) says that the convergent of the continued fraction expansion of ξ give the best rational approximations a/b to ξ if we want the denominator b to be small.

Proof

We will first show that (I) implies (II). Assume that

$$\left|\xi - \frac{a}{b}\right| < \left|\xi - \frac{h_n}{k_n}\right|$$

but $b \leq k_n$. Using the fact that $b/k_n \leq 1$, we conclude that

$$|\xi b - a| < \frac{b}{k_n}|\xi k_n - h_n| \leq |\xi k_n - h_n|$$

and $b \leq k_n \leq k_{n+1}$. This is a contradiction to (I) which has the conclusion that $b \geq k_{n+1}$.

To prove (I), suppose

$$|\xi b - a| < |\xi k_n - h_n|$$

for some $n \geq 0$ and $b < k_{n+1}$. Consider the equations in x and y:

$$xh_n + yh_{n+1} = a, \quad xk_n + yk_{n+1} = b.$$

By (11.1), we observe that

$$\det \begin{vmatrix} h_n & h_{n+1} \\ k_n & k_{n+1} \end{vmatrix} = \pm 1.$$

Hence, we conclude that x, y must be integers.

Note that if $x = 0$, then

$$y = \frac{b}{k_{n+1}} > 0,$$

or $y \geq 1$. This implies that $b \geq k_{n+1}$, a contradiction.

If $y = 0$, then $a = xh_n$ and $b = xk_n$. Hence,

$$|\xi b - a| = |\xi x k_n - x h_n| = |x||\xi k_n - h_n| \geq |k_n \xi - h_n|$$

since $|x| \geq 1$. This is a contradiction.

Next, we claim that $xy < 0$. If $y < 0$ then

$$xk_n = b - yk_{n+1}$$

shows that $x > 0$. If $y > 0$, then $b < k_{n+1}$ implies that

$$b < yk_{n+1}.$$

So $xk_n = b - yk_{n+1} < 0$ and therefore, $x < 0$.

Since the even convergents increase to ξ and the odd convergents decrease to ξ, we conclude that

$$\xi k_n - h_n \quad \text{and} \quad \xi k_{n+1} - h_{n+1}$$

have opposite signs. In other words, $x(\xi k_n - h_n)$ and $y(\xi k_{n+1} - h_{n+1})$ have the same sign and this implies that

$$|x(\xi k_n - h_n) + y(\xi k_{n+1} - h_{n+1})| = |x(\xi k_n - h_n)| + |y(\xi k_{n+1} - h_{n+1})|.$$

Finally, from the equations defining x and y, we deduce that

$$\begin{aligned} |\xi b - a| = |x(\xi k_n - h_n) + y(\xi k_{n+1} - h_{n+1})| &= |x(\xi k_n - h_n)| + |y(\xi k_{n+1} - h_{n+1})| \\ &\geq |x(\xi k_n - h_n)| \geq |\xi k_n - h_n|, \end{aligned}$$

which is a contradiction to our initial assumption.

□

EXAMPLE 11.1 It is well known that π is approximated by 22/7 and 355/113 (a number that is easy to remember by writing 113355 and splitting it as 113 and 355, with 355 as the numerator and 113 as the denominator). These numbers are the convergents for the continued fraction expansion of π, namely, $< 3, 7, 15, 1, 292, \cdots >$.

THEOREM 11.7 Let ξ denote any irrational number. If there is a rational number a/b with $b > 1$ and $(a, b) = 1$ such that

$$\left|\xi - \frac{a}{b}\right| < \frac{1}{2b^2},$$

then a/b equals to one of the convergents of the simple continued fraction of ξ.

Proof

Suppose a/b is not a convergent. Let n be such that

$$k_n \leq b < k_{n+1}. \tag{11.7}$$

For this choice of n, we find by Theorem 11.6 (I), that

$$|\xi k_n - h_n| \leq |\xi b - a| < \frac{1}{2b}.$$

This implies that

$$\left|\xi - \frac{h_n}{k_n}\right| < \frac{1}{2bk_n} \tag{11.8}$$

and

$$\left|\xi - \frac{a}{b}\right| < \frac{1}{2b^2}. \tag{11.9}$$

Since

$$\frac{a}{b} \neq \frac{h_n}{k_n},$$

the expression $bh_n - ak_n$ is a non-zero integer and we deduce, using (11.8) and (11.9), that

$$\frac{1}{bk_n} \leq \frac{|bh_n - ak_n|}{bk_n} = \left|\frac{h_n}{k_n} - \frac{a}{b}\right| \leq \left|\xi - \frac{h_n}{k_n}\right| + \left|\xi - \frac{a}{b}\right| < \frac{1}{2bk_n} + \frac{1}{2b^2}.$$

This implies that $b < k_n$, which contradicts (11.7). □

Suppose d is not a square and $d > 0$. We will show in this section that if

$$x^2 - dy^2 = 1$$

is solvable, then the solutions can be obtained from the continued fraction expansion of $\sqrt{d}$. [1]

Suppose

$$p^2 - dq^2 = 1.$$

Then

$$p^2 = 1 + dq^2 > dq^2.$$

Hence, $p > q$. Next, since $\sqrt{d} > 1$ and $p > q$, $p + \sqrt{d}q > q + q = 2q$.

Now,

$$p - \sqrt{d}q = \frac{1}{p + \sqrt{d}q} \leq \frac{1}{2q}.$$

Therefore, we find that

$$\frac{p}{q} - \sqrt{d} \leq \frac{1}{2q^2}.$$

By Theorem 11.7, we conclude that p/q must be a convergent of the continued fraction of $\sqrt{d}$.

REMARK 11.8 By studying periodic continued fraction, one can show that there exists non-zero positive integers x and y such that $x^2 - dy^2 = 1$. Moreover, if x_1 and y_1 are the smallest non-zero positive integers satisfying

$$x^2 - dy^2 = 1,$$

then all solutions with x, y positive are of the form

$$(x_1 + \sqrt{d}y_1)^n, n \in \mathbf{Z}^+.$$

11.6 The solvability of the Pell equation $x^2 - dy^2 = 1$ with $xy \neq 0$

In the last section, we see that all solutions to the Pell equation

$$x^2 - dy^2 = 1$$

can be obtained from the continued fraction expansion of $\sqrt{d}$ if the equation is solvable with $xy \neq 0$. In this section, we will prove that the equation is indeed solvable.

[1] It can be shown that the Pell equations can be solved if d is positive and squarefree.

DEFINITION 11.4 A continued fraction $< a_0, a_1, a_2, \cdots >$, where a_j are positive integers, is purely periodic if there exists a positive integer m such that

$$a_{m+k} = a_k,$$

for all integers $k \geq 0$.

We denote this as

$$< \overline{a_0, a_1, \cdots, a_{m-1}} > .$$

THEOREM 11.9 Let ξ be a real number. The continued fraction expansion of ξ is purely periodic if and only if ξ is a real quadratic irrational number ($\xi = u + v\sqrt{N}$ with $u, v \in \mathbf{Q}$, with N not a perfect square) satisfying $\xi > 1$ and $-1 < \xi' < 0$, where

$$\xi' = u - v\sqrt{N}.$$

REMARK 11.10 By real quadratic irrational number ξ, we mean $\xi \in \mathbf{Q}(\sqrt{N})$ for some positive integer N, where N is not a perfect square.

Proof

We will first prove that if $\xi > 1$ is a real quadratic irrational number and $-1 < \xi' < 0$, then ξ is purely periodic.

We will divide our proof into several steps.

Step 1.

Let $\xi = u + v\sqrt{N} = \dfrac{e}{f} + \dfrac{g}{h}\sqrt{N} = \dfrac{eh + gf\sqrt{N}}{fh}$. So we may write

$$\xi = \frac{a + b\sqrt{N}}{c},$$

with $a, b, c \in \mathbf{Z}$.

Note that since

$$\xi > 1 \quad \text{and} \quad -1 < \xi' < 0,$$

and this implies that

$$\frac{a}{c} + \frac{b}{c}\sqrt{N} > 1 \text{ and } -1 < \frac{a}{c} - \frac{b}{c}\sqrt{N} < 0.$$

By adding the inequalities, we conclude that $a/c > 0$. Similarly, by subtracting the inequalities, we conclude that $b/c > 0$. Multiplying both sides of the inequalities by c^2, we deduce that $ac > 0$ and $bc > 0$.

Therefore, we can write

$$\xi = \frac{m + \sqrt{M}}{q}$$

with $q = c^2 > 0$, $m = ac > 0$ and $M = (bc)^2 N$. Note that

$$M - m^2 = c^2(b^2 N) - c^2 a^2$$

is divisible by $c^2 = q$.

Step 2. Let

$$\xi = \xi_0 = \frac{m_0 + \sqrt{M}}{q_0},$$

where $q_0 = c^2$, $m_0^2 = a^2 q_0$, $M = q_0 b^2 N$. We observe that the following are true:

$$q_0 | (M - m_0^2), \xi_0 > 1, -1 < \xi_0' < 0, \, q_0 > 0, m_0 > 0. \tag{11.10}$$

Now, write

$$\xi_0 = a_0 + \frac{1}{\xi_1}. \tag{11.11}$$

Rearranging (11.11), we find that

$$\xi_1 = \frac{1}{\xi_0 - a_0} = \frac{(a_0 q_0 - m_0) + \sqrt{M}}{((M - (a_0 q_0 - m_0)^2)/q_0)}. \tag{11.12}$$

Now, $M - (a_0 q_0 - m_0)^2 = M - m_0^2 - (a_0 q_0)^2 + 2 a_0 q_0 m_0$ is divisible by q_0 since $q_0 | (M - m_0^2)$. So we may let

$$q_1 = \frac{M - m_1^2}{q_0}, \tag{11.13}$$

where

$$m_1 = a_0 q_0 - m_0 \tag{11.14}$$

Then we may now write

$$\xi_1 = \frac{m_1 + \sqrt{M}}{q_1}.$$

Note that the above discussion of $M - m_1^2$ shows that $q_1 | (M - m_1^2)$.

Next, $\xi_1 > 1$ by construction since

$$\xi_0 = a_0 + \frac{1}{\xi_1}.$$

Let σ be the automorphism of $\mathbf{Q}(\sqrt{M})$ such that

$$\sigma(\sqrt{M}) = -\sqrt{M}. \tag{11.15}$$

Applying σ to the second equality of (11.12), we deduce that

$$\xi_1' = \frac{1}{\xi_0' - a_0}.$$

Now, $a_0 \geq 1$ and so $-a_0 \leq -1$. By (11.10), $\xi_0' < 0$ and we conclude that

$$1/\xi_1' = \xi_0' - a_0 < -1.$$

and this implies that $\xi_1' > -1$. It is clear that $\xi_1' < 0$ since $-1/\xi_1' < 0$. Therefore the third condition of (11.16) is true. Using $\xi_1 = \dfrac{m_1 + \sqrt{M}}{q_1} > 1$ and $-1 < \xi_1' = \dfrac{m_1 - \sqrt{M}}{q_1} < 0$ and (11.12), we find that

$$\xi_1 - \xi_1' = 2\frac{\sqrt{M}}{q_1} > 0$$

or $q_1 > 0$. Next,

$$\xi_1 + \xi_1' = 2\frac{m_1}{q_1} > 0,$$

and since $q_1 > 0$, we conclude that $m_1 > 0$. Collecting what we have proved so far, we find that

$$q_1 | (M - m_1^2), \xi_1 > 1, -1 < \xi_1' < 0,\ q_1 > 0, m_1 > 0. \tag{11.16}$$

Step 3. We now define ξ_n, m_n, q_n recursively by

$$\xi_n = \frac{1}{\xi_{n-1} - a_{n-1}} = \frac{m_n + \sqrt{M}}{q_n},$$

where

$$a_{n-1} = [\xi_{n-1}],$$

$$m_n = a_{n-1}q_{n-1} - m_{n-1}$$

and

$$q_n q_{n-1} = M - m_n^2. \tag{11.17}$$

We want to show that for all positive integers n,

$$q_n | (M - m_n^2), \xi_n > 1, -1 < \xi_n < 0, q_n > 0, m_n > 0. \tag{11.18}$$

The statements in (11.18) can be established by induction and follows exactly the same steps when we deduce (11.16) from (11.10).

Step 4.

Now, by (11.18) and (11.17), we find that

$$0 < q_n \leq q_n q_{n-1} = M - m_n^2 \leq M.$$

Furthermore

$$0 < m_n^2 < m_n^2 + q_{n-1}q_n = M,$$

or

$$0 < m_n < \sqrt{M} < M.$$

Since M is fixed, we can only have finitely many possible pairs of values for (m_i, q_i). Therefore, there exist k and j with $k \neq j$ such that $m_j = m_k$ and $q_j = q_k$. This implies that

$$\xi_j = \xi_k$$

for some $j \neq k$.

Step 5. We now show that the continued fraction expansion of ξ is purely periodic. Applying σ to the definition of ξ_i, we find that for $i \geq 0$,

$$\xi_i' = a_i + \frac{1}{\xi_{i+1}'}.$$

We have seen from the second inequality of (11.18) that ξ_i' satisfies the inequality $-1 < \xi_i' < 0$ for all $i \geq 0$. Hence,

$$a_i < -\frac{1}{\xi_{i+1}'} < a_i + 1.$$

Therefore,

$$a_i = \left[-\frac{1}{\xi_{i+1}'}\right]. \tag{11.19}$$

Now, $\xi_j = \xi_k$ implies that

$$\xi_k' = \xi_j'$$

and

$$a_{j-1} = \left[-\frac{1}{\xi_j'}\right] = \left[-\frac{1}{\xi_k'}\right] = a_{k-1}.$$

Hence

$$\xi_{j-1} = a_{j-1} + \frac{1}{\xi_j} = a_{k-1} + \frac{1}{\xi_k} = \xi_{k-1}.$$

Hence, $\xi_j = \xi_k$ implies that $\xi_{j-1} = \xi_{k-1}$. By continuing the above process, we observe that

$$\xi_{j-r} = \xi_{k-r}$$

for $0 < r < \min(j, k)$. If $k > j$, then we conclude that

$$\xi_{k-j} = \xi_0 = \xi.$$

Hence, we may write

$$\xi = < \overline{a_0, a_1, \cdots, a_{k-j-1}} >$$

and the proof is complete.

To prove the converse, we let ξ be a real number and assume that the continued fraction expansion of ξ is purely periodic, say,

$$\xi = < \overline{a_0, a_1, \cdots, a_{n-1}} > .$$

By definition $a_0 \geq 1$ and so, $\xi \geq 1$. If ξ were rational, say u/v then by Euclidean

Algorithm the continued fraction expansion of ξ is finite and therefore cannot be purely periodic.

Next, from the continued fraction expansion of ξ, we find, by Theorem 11.1, that

$$\xi = \frac{\xi h_{n-1} + h_{n-2}}{\xi k_{n-1} + k_{n-2}}.$$

From the above equation and the fact that ξ is not rational, we conclude that ξ is a irrational real quadratic number. Note that since $a_0 \geq 1$, $\xi > 1$.

Let

$$f(x) = x^2 k_{n-1} + x(k_{n-2} - h_{n-1}) - h_{n-2}.$$

Then $f(\xi) = 0$. By applying the map σ given by (11.15) to $f(\xi)$, we observe that

$$0 = \sigma(0) = f(\sigma(\xi)) = f(\xi').$$

Hence, ξ' is also a zero of $f(x)$. Next, note that $f(0) = -h_{n-2} < 0$ and

$$f(-1) = k_{n-1} - k_{n-2} + h_{n-1} - h_{n-2} > 0$$

since both $\{h_n\}$ and $\{k_n\}$ are increasing. Therefore, by intermediate value theorem, $f(x)$ has a zero between -1 and 0. Since the zeroes of $f(x)$ are ξ and ξ' and that $\xi > 1$, we conclude that $-1 < \xi' < 0$. □

REMARK 11.11 We can prove that

$$\xi_1 = \frac{1}{\xi_0 - a_0}$$

implies that

$$\xi_1' = \frac{1}{\xi_0' - a_0}$$

without using the field automorphism σ. It suffices to show that if

$$u + v\sqrt{d} = \frac{1}{a + b\sqrt{d}},$$

then

$$u - v\sqrt{d} = \frac{1}{a - b\sqrt{d}}.$$

From the first equation, we deduce that

$$ua + bvd + (va + ub)\sqrt{d} = 1.$$

Since 1 and $\sqrt{d}$ are linearly independent over $\mathbf{Q}$, i.e., $s + t\sqrt{d} = 0, s, t \in \mathbf{Q}$ implies that $s = t = 0$, we conclude that $va + ub = 0$. Therefore

$$ua + bvd - (va + ub)\sqrt{d} = 1$$

and this implies, by reversing what we did in the beginning, that

$$u - v\sqrt{d} = \frac{1}{a - b\sqrt{d}},$$

which is what we want to show.

COROLLARY 11.12 The number $\sqrt{d}+[\sqrt{d}]$ is purely periodic.

Proof
The results follow immediately from Theorem 11.9 by checking that

$$\sqrt{d}+[\sqrt{d}]>1$$

and

$$-1<[\sqrt{d}]-\sqrt{d}<0.$$

□

THEOREM 11.13 If

$$\sqrt{d}+[\sqrt{d}]=<a_0,a_1,\cdots,\xi_n>,$$

and

$$\sqrt{d}=<[\sqrt{d}],a_1,\cdots,\eta_n>,$$

then

$$\xi_n=\eta_n$$

for all integers $n\geq 1$.

Proof
Note that if $\{\sqrt{d}\}=\sqrt{d}-[\sqrt{d}]$ then

$$\frac{1}{\{\sqrt{d}\}}=<a_1,a_2,\cdots,a_{n-1},\eta_n>.$$

But $\{\sqrt{d}\}=\sqrt{d}+[\sqrt{d}]-a_0=\sqrt{d}+[\sqrt{d}]-2[\sqrt{d}]$ and

$$\frac{1}{\{\sqrt{d}\}}=<a_1,a_2,\cdots,a_{n-1},\xi_n>.$$

This implies that for $n\geq 1$, $\xi_n=\eta_n$. □

THEOREM 11.14 If d is a positive integer that is not a perfect square, then

$$h_n^2-dk_n^2=(-1)^{n-1}q_{n+1}$$

for all integers $n\geq -1$, where

$$\xi_{n+1}=\frac{m_{n+1}+\sqrt{d}}{q_{n+1}}.$$

Proof
Let $n \geq 0$. We first note that if h_n/k_n is the n-th convergent of $\sqrt{d}$, then by Theorem 11.1,

$$\begin{aligned}\sqrt{d} &= \frac{\eta_{n+1}h_n + h_{n-1}}{\eta_{n+1}k_n + k_{n-1}} \\ &= \frac{\xi_{n+1}h_n + h_{n-1}}{\xi_{n+1}k_n + k_{n-1}} \\ &= \frac{(m_{n+1} + \sqrt{d})h_n + q_{n+1}h_{n-1}}{(m_{n+1} + \sqrt{d})k_n + q_{n+1}k_{n-1}},\end{aligned} \tag{11.20}$$

where we have used the representation

$$\xi_{n+1} = \frac{m_{n+1} + \sqrt{d}}{q_{n+1}}$$

and Theorem 11.13, which expresses η_n in terms of ξ_n for $n \geq 1$. From (11.20), we deduce that

$$\sqrt{d}(m_{n+1}k_n + q_{n+1}k_{n-1}) + dk_n = \sqrt{d}h_n + (m_{n+1}h_n + q_{n+1}h_{n-1}). \tag{11.21}$$

Next, 1 and $\sqrt{d}$ are linearly independent over $\mathbf{Q}$ (see the remark after Theorem 11.9. Using this observation and (11.21), we conclude that

$$h_n = m_{n+1}k_n + q_{n+1}k_{n-1},$$

and

$$dk_n = m_{n+1}h_n + q_{n+1}h_{n-1}.$$

Therefore,

$$h_n^2 - dk_n^2 = h_n(m_{n+1}k_n + q_{n+1}k_{n-1}) - k_n(m_{n+1}h_n + q_{n+1}h_{n-1}) = (-1)^{n-1}q_{n+1},$$

since

$$k_{n-1}h_n - h_{n-1}k_n = (-1)^{n-1},$$

by (11.1). □

Now, if

$$\sqrt{d} + [\sqrt{d}] = < \overline{a_0, a_1, a_2, \cdots, a_{r-1}} >,$$

with $a_0 = 2[\sqrt{d}]$ then

$$\xi_{nr} = \xi_r.$$

But for $m > 1$, $\xi_m = \eta_m$ and hence

$$\eta_{nr} = \eta_r$$

for $n \geq 1$.

Note that since

$$\xi_0 = \xi_r = \eta_r = [\sqrt{d}] + \sqrt{d},$$

we conclude that $q_0 = q_r = 1$. Hence $q_{nr} = 1$ for all integers $n \geq 1$. Therefore,

$$h_{2nr-1}^2 - dk_{2nr-1}^2 = 1. \tag{11.22}$$

This shows that the Pell equation is always solvable in x and y with $xy \neq 0$.

We note that if the period r is even, then we may replace $2n$ by n in (11.22) to obtain

$$h_{nr-1}^2 - dk_{nr-1}^2 = 1. \tag{11.23}$$

EXAMPLE 11.2 The continued fraction expansion of $\sqrt{3} + [\sqrt{3}]$ is

$$< \overline{2, 1} > .$$

Here $r = 2$. The continued fraction expansion of $\sqrt{3}$ is $< 1, 1, 2, 1, 2, \cdots >$. By (11.23), $\dfrac{h_1}{k_1} = \dfrac{2}{1}$ and it is immediate that $x = 2$ and $y = 1$ is a solution of $x^2 - 3y^2 = 1$.

12 Jacobi's Triple Product Identity and the partition function $p(n)$

12.1 Jacobi's Triple Product Identity

Let $r_2(n)$ be the number of ways of writing n as a sum of two squares. If we can prove that $r_2(p) > 0$ when $p \equiv 1 \pmod 4$, then we would have proved that p can be expressed as a sum of two squares. But can we do that? The answer is "yes".

Let

$$\Theta(q) = \sum_{j=-\infty}^{\infty} q^{j^2}.$$

Observe that

$$\Theta^2(q) = \sum_{j=-\infty}^{\infty} \sum_{k=-\infty}^{\infty} q^{j^2+k^2} = \sum_{n=0}^{\infty} r_2(n) q^n. \tag{12.1}$$

We will derive a formula for $r_2(n)$ by studying the function $\Theta(q)$.

12.2 The terminating q-binomial Theorem

Let $n \geq 1$ be an integer. The binomial theorem states that

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k \tag{12.2}$$

where

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}. \tag{12.3}$$

There is a q-analogue of (12.2) and to describe this analogue, we first define the q-analogue of (12.3).

DEFINITION 12.1 Let $(q)_0 = 1$ and let

$$(q)_n = \prod_{j=1}^{n} (1-q^j)$$

and

$$\begin{bmatrix} n \\ k \end{bmatrix}_n = \frac{(q)_n}{(q)_k (q)_{n-k}}. \tag{12.4}$$

We also let

$$(q)_\infty = \prod_{k=1}^{\infty} (1 - q^k).$$

The expression in (12.4) is a q-analogue of (12.3) since

$$\begin{aligned} \lim_{q \to 1^-} \begin{bmatrix} n \\ k \end{bmatrix}_q &= \lim_{q \to 1^-} \frac{(1-q)(1-q^2)\cdots(1-q^n)}{(1-q)^n} \cdot \frac{(1-q)^k}{(q)_k} \cdot \frac{(1-q)^{n-k}}{(q)_{n-k}} \\ &= \binom{n}{k}. \end{aligned}$$

Observe further that the expressions for (12.3) and (12.4) motivate us to view the q-analogue of $n!$ as $(q)_n$, even though $(q)_n$ does not approach $n!$ as q approaches 1^-.

The q-binomial coefficient has several interesting properties. For example, one can verify that

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = q^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q \tag{12.5}$$

and

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n-1 \\ k \end{bmatrix}_q + q^{n-k} \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q. \tag{12.6}$$

When q approaches 1^-, both (12.5) and (12.6) reduce to the well known relation

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

By (12.5), (12.6) and mathematical induction, we deduce that $\begin{bmatrix} n \\ k \end{bmatrix}_q$ is a polynomial in q. This is analogous to the fact that $\binom{n}{k}$ is an integer.

We are now ready to establish the following analogue of (12.2):

THEOREM 12.1 Let n be a positive integers, x and q be independent variables. Then

$$(1+x)(1+xq)\cdots(1+xq^{n-1}) = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q q^{k(k-1)/2} x^k. \tag{12.7}$$

Proof
We follow the approach of G. Polya and G.L. Alexanderson Denote

$$f(x) = (1+x)(1+xq)\cdots(1+xq^{n-1}).$$

Note that

$$\begin{aligned}(1+x)f(xq) &= (1+x)(1+xq)\cdots(1+xq^{n-1})(1+xq^n)\\ &= f(x)(1+xq^n).\end{aligned}$$

If we write

$$f(x) = \sum_{k=0}^{n} Q_k x^k,$$

where Q_k is a function of q, then

$$(1+x)\left(\sum_{k=0}^{n} q^k Q_k x^k\right) = (1+xq^n)\left(\sum_{k=0}^{n} Q_k x^k\right).$$

Comparing the coefficient of x^k on both sides, we deduce that

$$q^k Q_k + q^{k-1}Q_{k-1} = Q_k + q^n Q_{k-1},$$

which implies that

$$(1-q^k)Q_k = q^{k-1}(1-q^{n-k+1})Q_{k-1}.$$

Hence, we find that

$$Q_k = q^{k-1}\frac{(1-q^{n-k+1})}{(1-q^k)}Q_{k-1}. \tag{12.8}$$

Observing that $Q_0 = 1$ and iterating (12.8), we deduce that

$$\begin{aligned}Q_k &= q^{(k-1)+(k-2)+\cdots 2+1}\frac{(1-q^{n-k+1})(1-q^{n-k+2})\cdots(1-q^n)}{(1-q^k)(1-q^{k-1})\cdots(1-q^2)(1-q)}Q_0\\ &= q^{k(k-1)/2}\begin{bmatrix} n \\ k \end{bmatrix}_q.\end{aligned}$$

This completes the proof of (12.7). □

12.3 The Jacobi Triple Product Identity

In this section, we prove the following theorem:

THEOREM 12.2 Let q and z be complex numbers such that $|q| < 1$. Then

$$\sum_{j=-\infty}^{\infty} q^{j^2} z^j = \prod_{j=1}^{\infty}(1+zq^{2j-1})(1+z^{-1}q^{2j-1})(1-q^{2j}). \tag{12.9}$$

REMARK 12.3 Identity (12.9) is known as the Jacobi Triple Product Identity.

Before we give the proof of (12.9), we give two special cases of the identity.

EXAMPLE 12.1 Let $z = q$ in (12.9), followed by replacing q by $q^{1/2}$. We find that

$$\sum_{j=-\infty}^{\infty} q^{j(j+1)/2} = 2\prod_{j=1}^{\infty}(1+q^j)^2(1-q^j).$$

EXAMPLE 12.2 Let q be replaced by $q^{3/2}$, followed by letting $z = -q^{1/2}$. We immediately deduce from (12.9) that

$$\sum_{j=-\infty}^{\infty}(-1)^j q^{j(3j+1)/2} = \prod_{j=1}^{\infty}(1-q^{3j-1})(1-q^{3j-2})(1-q^{3j}) = \prod_{j=1}^{\infty}(1-q^j), \quad (12.10)$$

where the last equality follows from the fact that a positive integer must be of the form $3j - r$, with $r = 0, 1$ or 2.

Proof

Let $n = 2N$ in (12.7) and note that

$$(1+x)\cdot(1+qx)\cdot(1+q^2x)\cdots(1+q^{2N-1}x) = \sum_{j=0}^{2N}\frac{(1-q^{2N})(1-q^{2N-1})\cdots(1-q^{2N-j+1})}{(1-q)(1-q^2)\cdots(1-q^j)}q^{j(j-1)/2}x^j.$$

Next, replace x by $q^{-N}x$ and we find that

$$(1+q^{-N}x)\cdot(1+q^{-N+1}x)\cdot(1+q^{-N+2}x)\cdots(1+q^{N-1}x) = \sum_{j=0}^{2N}\frac{(1-q^{2N})(1-q^{2N-1})\cdots(1-q^{2N-j+1})}{(1-q)(1-q^2)\cdots(1-q^j)}q^{j(j-1)/2}q^{-Nj}x^j$$

Let $j = N + \ell$ on the right hand side and deduce that

$$\begin{aligned}
&(1+q^{-N}x)\cdot(1+q^{-N+1}x)\cdot(1+q^{-N+2}x)\cdots(1+q^{N-1}x)\\
&= \sum_{\ell=-N}^{N}\frac{(1-q^{2N})(1-q^{2N-1})\cdots(1-q^{N-\ell+1})}{(1-q)(1-q^2)\cdots(1-q^{N+\ell})}q^{(N+\ell)((N+\ell)-1)/2}q^{-N(N+\ell)}x^{\ell+N}\\
&= \sum_{\ell=-N}^{N}\frac{(1-q^{2N})(1-q^{2N-1})\cdots(1-q^{N-\ell+1})}{(1-q)(1-q^2)\cdots(1-q^{N+\ell})}q^{(N^2+\ell^2+2N\ell-N-\ell)/2}q^{-N^2-N\ell}x^{\ell+N}\\
&= \sum_{\ell=-N}^{N}\frac{(1-q^{2N})(1-q^{2N-1})\cdots(1-q^{N-\ell+1})}{(1-q)(1-q^2)\cdots(1-q^{N+\ell})}q^{-N^2/2-N/2+\ell^2/2-\ell/2}x^{\ell+N}.
\end{aligned}$$

Multiplying both sides by $x^{-N}q^{N(N+1)/2}$ and simplifying, we conclude that

$$(1+q^N/x)(1+q^{N-1}/x)\cdots(1+q/x)(1+x)(1+qx)\cdots(1+q^{N-1}x)$$
$$=\sum_{\ell=-N}^{N}\frac{(1-q^{2N})(1-q^{2N-1})\cdots(1-q)}{(1-q)(1-q^2)\cdots(1-q^{N+\ell})(1-q)(1-q^2)\cdots(1-q^{N-\ell})}q^{\ell(\ell-1)/2}x^\ell.$$

Letting $N\to\infty$, we deduce that

$$\prod_{k=1}^{\infty}(1-q^k)(1+q^k/x)(1+q^{k-1}x)=\sum_{\ell=-\infty}^{\infty}q^{\ell(\ell-1)/2}x^\ell. \tag{12.11}$$

Replacing q by q^2 and x by qx, we complete the proof of (12.9). □

REMARK 12.4 In the above proof, the replacement of N by ∞ can be justified by Tannery's Theorem. The above proof is known to Gauss (1866) and Cauchy (1843).

12.4 Jacobi's triple product identity and sums of two squares

In this section, we will use Jacobi's triple product identity to derive the following identity:

THEOREM 12.5 Let $|q|<1$. Then

$$1+\sum_{n=1}^{\infty}r_2(n)q^n=\Theta^2(q)=1+4\left(\sum_{j=1}^{\infty}\frac{q^{4j-3}}{1-q^{4j-3}}-\frac{q^{4j-1}}{1-q^{4j-1}}\right).$$

We give the proof which is due to M. Hirschhorn.

Proof
Replace z by $-x^2q$ and q^2 by q in (12.9) to deduce that

$$(x-x^{-1})\prod_{k=1}^{\infty}(1-x^2q^k)(1-x^{-2}q^k)(1-q^k)=\sum_{k=-\infty}^{\infty}(-1)^kx^{2k+1}q^{k(k+1)/2}. \tag{12.12}$$

We now set $k=2n$ and $k=2n+1$ in the sum on the right hand side and deduce that

$$(x-x^{-1})\prod_{k=1}^{\infty}(1-x^2q^k)(1-x^{-2}q^k)(1-q^k)$$
$$=\sum_{n=-\infty}^{\infty}x^{4n+1}q^{2n^2+n}-\sum_{n=-\infty}^{\infty}x^{4n-1}q^{2n^2-n}$$
$$=:E(x)-O(x), \tag{12.13}$$

where

$$E(x) = \sum_{n=-\infty}^{\infty} x^{4n+1} q^{2n^2+n}$$

and

$$O(x) = \sum_{n=-\infty}^{\infty} x^{4n-1} q^{2n^2-n}.$$

Using (12.9), we deduce that

$$E(x) = x \sum_{j=-\infty}^{\infty} q^{2j^2+j} x^{4j} = x \prod_{k=1}^{\infty} (1 + x^4 q^{4k-1})(1 + x^{-4} q^{4k-3})(1 - q^{4k}) \quad (12.14)$$

and

$$O(x) = x^{-1} \sum_{j=-\infty}^{\infty} q^{2j^2-j} x^{4j} = x^{-1} \prod_{k=1}^{\infty} (1 + x^4 q^{4k-3})(1 + x^{-4} q^{4k-1})(1 - q^{4k}). \quad (12.15)$$

We next differentiate both sides of (12.13) with respect to x and set $x = 1$. Let

$$L(x) = (x - x^{-1}) \prod_{k=1}^{\infty} (1 - x^2 q^k)(1 - x^{-2} q^k)(1 - q^k) = x - x^{-1}) P(x).$$

Then

$$L'(x) = (x - x^{-1}) P'(x) + (1 + x^{-2}) P(x).$$

This implies that

$$L'(1) = 2P(1) = 2 \prod_{k=1}^{\infty} (1 - q^k)^3. \quad (12.16)$$

For the right-hand-side, we obtain $E'(x)$ and $O'(x)$ by logarithmically differentiating the product representations of $E(x)$ and $O(x)$. For the function $E(x)$, we find that

$$\ln E(x) = \ln x + \sum_{j=1}^{\infty} \ln(1 + x^4 q^{4j-1}) + \sum_{j=1}^{\infty} \ln(1 + x^{-4} q^{4j-3}) + \sum_{j=1}^{\infty} \ln(1 - q^{4j}),$$

which implies that

$$E'(x) = E(x) \left(\frac{1}{x} + \sum_{j=1}^{\infty} \frac{4x^3 q^{4j-1}}{1 + x^4 q^{4j-1}} - \sum_{j=1}^{\infty} \frac{4x^{-5} q^{4j-3}}{1 + x^{-4} q^{4j-3}} \right).$$

Therefore,

$$E'(1) = \prod_{k=1}^{\infty} (1+q^{4k-1})(1+q^{4k-3})(1-q^{4k}) \left(1 + 4 \sum_{j=1}^{\infty} \frac{q^{4j-1}}{1 + q^{4j-1}} - 4 \sum_{j=1}^{\infty} \frac{q^{4j-3}}{1 + q^{4j-3}} \right). \quad (12.17)$$

Similarly,

$$O'(1) = \prod_{k=1}^{\infty}(1+q^{4k-1})(1+q^{4k-3})(1-q^{4k}) \left(-1 + 4\sum_{j=1}^{\infty} \frac{q^{4j-3}}{1+q^{4j-3}} - 4\sum_{j=1}^{\infty} \frac{q^{4j-1}}{1+q^{4j-1}} \right). \tag{12.18}$$

Combining (12.16), (12.17) and (12.18), we conclude that

$$2\prod_{k=1}^{\infty}(1-q^k)^3 = 2\prod_{k=1}^{\infty}(1+q^{4k-1})(1+q^{4k-3})(1-q^{4k}) \left(1 + 4\sum_{j=1}^{\infty} \frac{q^{4j-1}}{1+q^{4j-1}} - 4\sum_{j=1}^{\infty} \frac{q^{4j-3}}{1+q^{4j-3}} \right).$$

Simplifying the above identity using the identities

$$\begin{aligned} \prod_{k=1}^{\infty}(1+q^{4k-1})(1+q^{4k-3})(1-q^{4k}) &= \prod_{k=1}^{\infty}(1+q^{2k-1})(1-q^{4k}) \\ &= \prod_{k=1}^{\infty} \frac{(1-q^{4k-2})}{(1-q^{2k-1})}(1-q^{4k}) \\ &= \prod_{k=1}^{\infty} \frac{(1-q^{2k})}{(1-q^{2k-1})} \end{aligned}$$

and

$$\begin{aligned} \prod_{k=1}^{\infty} \frac{(1-q^k)^3}{(1+q^{4k-1})(1+q^{4k-3})(1-q^{4k})} &= \prod_{k=1}^{\infty} \frac{(1-q^k)^3(1-q^{2k-1})}{(1-q^{2k})} \\ &= \prod_{k=1}^{\infty} \frac{(1-q^{2k})^3(1-q^{2k-1})^3(1-q^{2k-1})}{(1-q^{2k})} \\ &= \prod_{k=1}^{\infty}(1-q^{2k-1})^4(1-q^{2k})^2, \end{aligned}$$

we deduce that

$$\prod_{k=1}^{\infty}(1-q^{2k-1})^4(1-q^{2k})^2 = 1 + 4\sum_{j=1}^{\infty} \frac{q^{4j-1}}{1+q^{4j-1}} - 4\sum_{j=1}^{\infty} \frac{q^{4j-3}}{1+q^{4j-3}}.$$

We next replace q by $-q$ and use (12.9) to deduce that

$$\Theta(q) = \prod_{k=1}^{\infty}(1+q^{2k-1})^2(1-q^{2k})$$

and that

$$\Theta^2(q) = \prod_{k=1}^{\infty}(1+q^{2k-1})^4(1-q^{2k})^2.$$

This implies that

$$1 + \sum_{n=1}^{\infty} r_2(n)q^n = \Theta^2(q) = 1 + 4\sum_{j=1}^{\infty} \frac{q^{4j-3}}{1-q^{4j-3}} - 4\sum_{j=1}^{\infty} \frac{q^{4j-1}}{1-q^{4j-1}}.$$

Therefore,

$$\begin{aligned}1+\sum_{n=1}^{\infty} r_2(n)q^n &= 1+4\sum_{n=1}^{\infty}\left(\frac{q^{4n-3}}{1-q^{4n-3}}-\frac{q^{4n-1}}{1-q^{4n-1}}\right)\\ &= 1+4\sum_{n=1}^{\infty}\sum_{m=1}^{\infty}\left(q^{(4n-3)m}-q^{(4n-1)m}\right)\\ &= 1+4\sum_{n=1}^{\infty}\left(\sum_{\substack{d|n\\ d\equiv 1(\mathrm{mod}\ 4)}} 1-\sum_{\substack{d|n\\ d\equiv 3(\mathrm{mod}\ 4)}} 1\right)q^n.\end{aligned}$$

□

We are now ready to show that $r_2(p) > 0$ if p is a prime of the form $4k+1$. Note that if p is of the form $4k+1$ then the two divisors of p, namely, 1 and p, are both of the form $4k+1$. Therefore

$$r_2(p) = 8 > 0,$$

using the formula for $r_2(n)$. This completes the proof that p must be of the form x^2+y^2.

12.5 The Partition Function $p(n)$ and its Generating Function

DEFINITION 12.2 A partition of a positive integer n is a representation of n as a sum of non-decreasing positive integers, called summands or parts of the partition. The partition function $p(n)$ is defined as the number of partitions of n.

The function $p(n)$ is not defined for $n = 0$ but we will set $p(0) = 1$.

EXAMPLE 12.3 *The integer* 4 *has the following partitions.*

$$4 = 1+3 = 2+2 = 1+1+2 = 1+1+1+1.$$

The number of partitions of 4 *is 5 and we write* $p(4) = 5$.

One of the most important identities associated with $p(n)$ is the following.

THEOREM 12.6 *For* $|q| < 1$, *we have*

$$\prod_{k=1}^{\infty}\frac{1}{(1-q^k)} = \sum_{n=0}^{\infty} p(n)q^n. \tag{12.19}$$

REMARK 12.7 See the book by G.H. Hardy and E.M. Wright for a rigorous proof of the above theorem.

Observe from Theorem 12.6 that

$$1 = \prod_{k=1}^{\infty}(1-q^k)\sum_{n=0}^{\infty}p(n)q^n.$$

Using (12.10), we find that

$$\begin{aligned}1 &= \left(1+\sum_{\nu=1}^{\infty}(-1)^{\nu}(q^{\nu(3\nu+1)/2}+q^{\nu(3\nu-1)/2})\right)\sum_{j=0}^{\infty}p(j)q^j\\ &= \left(1+\sum_{\mu=0}^{\infty}(-1)^{\mu+1}(q^{(\mu+1)(3\mu+2)/2})+q^{(\mu+1)(3\mu+4)/2}\right)\sum_{j=0}^{\infty}p(j)q^j.\end{aligned}$$

Hence, we deduce that for $N \geq 1$,

$$p(N) = \sum_{\substack{j,\mu\geq 0\\ j+\frac{(\mu+1)(3\mu+2)}{2}=N}}(-1)^{\mu}p(j) + \sum_{\substack{j,\mu\geq 0\\ j+\frac{(\mu+1)(3\mu+4)}{2}=N}}(-1)^{\mu}p(j). \tag{12.20}$$

Major MacMahon, using (12.20), tabulated $p(n)$ up to $n = 200$.

S. Ramanujan was the first mathematician to notice that there might be a formula for determining $p(n)$ directly without using the recurrence (12.20). Around 1918, Ramanujan and G.H. Hardy succeeded in expressing $p(n)$ as the integer part of a finite sum which diverges as the upper index of the summation tends to ∞. In 1937, H. Rademacher discovered an exact formula of $p(n)$ in terms of a convergent series. A. Selberg had also independently discovered the same formula around the same time.

12.6 Ramanujan's Congruences for $p(n)$

According to G.H. Hardy, S. Ramanujan was led to three striking congruences satisfied by $p(n)$ when examining MacMahon's table of $p(n)$.

Ramanujan's first congruence is stated in the following theorem.

THEOREM 12.8 *Let n be a positive integer. Then*

$$p(5n-1) \equiv 0 \pmod 5. \tag{12.21}$$

Proof We use (12.10) and (12.16) to deduce that

$$\begin{aligned}q\prod_{k=1}^{\infty}(1-q^k)^4 &= q\prod_{k=1}^{\infty}(1-q^k)\prod_{k=1}^{\infty}(1-q^k)^3\\ &= \sum_{r=-\infty}^{\infty}\sum_{s=0}^{\infty}(-1)^{r+s}(2s+1)q^{1+r(3r+1)/2+s(s+1)/2}.\end{aligned}$$

Observe that when

$$1 + r(3r+1)/2 + s(s+1)/2$$

is a multiple of 5, then

$$2 + 3r^2 + r + s^2 + s \equiv 0 \pmod 5.$$

Multiplying both sides by 4, we conclude that

$$3 + 2r^2 + 4r + 4s^2 + 4s \equiv 0 \pmod 5,$$

which implies that

$$2(r+1)^2 + (2s+1)^2 \equiv 0 \pmod 5. \tag{12.22}$$

Now, we find that

$$2M^2 + N^2 \equiv 0 \pmod 5$$

has a solution if

$$N^2 \equiv -2M^2 \pmod 5. \tag{12.23}$$

If $M \not\equiv 0 \pmod 5$, then (12.23) implies that NM^{-1} is a solution of

$$x^2 \equiv -2 \pmod 5.$$

This is false since -2 is not a quadratic residue modulo 5. Hence, if (12.23) holds, we must have

$$M \equiv 0 \pmod 5$$

and

$$N \equiv 0 \pmod 5.$$

Returning to (12.22), we observe that if (12.22) holds, then

$$2s + 1 \equiv 0 \pmod 5. \tag{12.24}$$

If we write

$$q \prod_{n=1}^{\infty} (1-q^n)^4 = \sum_{j=0}^{\infty} a_j q^j,$$

then the coefficient of q^{5j} in the above expansion is given by

$$a_{5j} = \sum_{\substack{r,s=-\infty \\ 1+r(3r+1)/2+s(s+1)/2=5j}}^{\infty} (-1)^{r+s}(2s+1) \equiv 0 \pmod 5, \tag{12.25}$$

where our last congruence follows from (12.24).

Next, we recall that if $f(q)$ and $g(q)$ are two power series with integral coefficients, then for any prime p, we write

$$f(q) \equiv g(q) \pmod p$$

if

$$f(q) - g(q) = ph(q)$$

for some power series $h(q)$ with integral coefficients. Observe that

$$1 - q^{5n} \equiv (1 - q^n)^5 \pmod 5$$

and this implies that

$$q \prod_{n=1}^{\infty} \frac{(1 - q^{5n})}{(1 - q^n)} \equiv q \prod_{n=1}^{\infty} (1 - q^n)^4 \pmod 5.$$

Thus, by (12.19), we deduce that

$$\begin{aligned} \sum_{k=0}^{\infty} p(k) q^{k+1} &\equiv \sum_{j=0}^{\infty} a_j q^j \prod_{\ell=1}^{\infty} \frac{1}{1 - q^{5\ell}} \\ &\equiv \sum_{j=0}^{\infty} a_j q^j \sum_{\ell=0}^{\infty} p(\ell) q^{5\ell} \pmod 5. \end{aligned} \tag{12.26}$$

Comparing coefficients of q^{5m} on both sides of (12.26), we conclude that

$$p(5m - 1) \equiv \sum_{5j+5\ell=5m} a_{5j} p(\ell) \equiv 0 \pmod 5,$$

where the last congruence follows from (12.25).

□

Besides (12.21), Ramanujan also discovered the congruences

$$p(7n - 2) \equiv 0 \pmod 7 \tag{12.27}$$

and

$$p(11n - 5) \equiv 0 \pmod{11}. \tag{12.28}$$

The proof of (12.27) is similar to the proof of (12.21).

REMARK 12.9 In order to give a proof similar to Ramanujan's method for (12.28), one would need to consider the series expansion of $\prod_{k=1}^{\infty}(1 - q^k)^{10}$. Ramanujan did not have a series representation of the above product. This was provided by L. Winquist. He showed that

$$\begin{aligned} \prod_{k=1}^{\infty} (1 - q^k)^{10} = \sum_{\nu=-\infty}^{\infty} \sum_{\mu=-\infty}^{\infty} (-1)^{\nu+\mu} (2\nu + 1)(6\mu + 1) \\ \left(\frac{(3\nu + 1)(3\nu + 2)}{4} - \frac{3\mu(3\mu + 1)}{4} \right) q^{3\nu(\nu+1)/2 + \mu(3\mu+1)/2} \end{aligned} \tag{12.29}$$

and provided the first published proof of (12.28) in the spirit of Ramanujan's proof of (12.21) and (12.27). Winquist's identity (12.29) can be interpreted as a special case of Macdonald's identity for twisted affine Kac-Moody algebras.